efl insights 02|2021

An efl – the Data Science Institute Publication

efl the Data Science Institute

Data Democratization in Asset Management

Jump on the Hype – German Retail Investors and the Gamestop Frenzy

Phish Me If You Can: Insights from an Eye-Tracking Experiment

Is Platform Lending Just a Flash in the Pan?

DEUTSCHE BÖRSE GROUP | DZ BANK Gruppe | finanz informatik
AMERICAN EXPRESS | Deutsche Leasing | FACTSET

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

TECHNISCHE UNIVERSITÄT DARMSTADT

Impressum

Redaktion
Prof. Dr. Peter Gomber
Dr. Jascha-Alexander Koch

Herausgeber
Prof. Dr. Wolfgang König
Vorstandsvorsitzender
efl – the Data Science Institute e. V.

Prof. Dr. Peter Gomber
Stellvertretender Vorstandsvorsitzender
efl – the Data Science Institute e. V.

Kontakt
info@eflab.de
www.eflab.de

Gestaltung
Novensis Communication GmbH
Bad Homburg

2. Ausgabe, 2021
Auflage: 200 Stück (Print) / 2.000 Stück (E-Paper)

Printed in Germany
ISSN 1866-1238

Editorial

Data Democratization in Asset Management

Markus Lohmann

Dr. Markus Lohmann
Chief Technology and Data Officer
Allianz Global Investors

"Data is the new oil" is the claim often used to underpin the importance of data for business progress. In fact, in May 2017, The Economist reported that the world's most valuable resource is no longer oil, but data. But how can we effectively make use of data, in particular in regulated industries such as asset management?

The Traditional Way of Data Processing in Asset Management

Today, the "need-to-know principle" is the dominant principle to grant access to data within the investment and asset management industry. Requesting access to sources actively is the norm and, hence, only well-planned cross-functional data combinations (e.g., distribution inflow/outflow data linked to marketing campaign data) are analyzed, which leaves many insights uncovered. The blind spots stay huge while compliance functions are happy as this approach brings the easiest way to achieve regulatory (and business) compliance.

Data Democratization as the Current Paradigm

At Allianz Global Investors, we have turned the "need-to-know" principle upside down and implemented "Data Democratization" as our new access paradigm. All internal and external data sets are accessible by default by all employees, restrictions driven by regulation, like data privacy or license coverage, are applied nevertheless and are the only valid reasons for denied access.

Now, it's much easier to, e.g., link portfolio/trade data, flow data, and input from marketing campaigns with third parties, e.g., sentiment data. Blind spots are becoming smaller and so-far hidden linkages of datasets become visible and generate new insights. This sounds easy but raises the question on how the semantics of the combined datasets remain meaningful and fit for purpose, so that, e.g., any client report is using settled trade data and not unsettled trade data.

Using Democratized Data Effectively Requires Strong Governance and Architectures

Data governance delivers most of the answers. While loads of combinations of datasets are technically feasible, it requires quality-driven modeling to create business-friendly views and a governance check whether the semantics of the combined sets are fit for purpose. Strict use of data dictionaries and catalogs facilitates exploring datasets. An approval process between users and owners of the datasets ensures that the intended use is semantically viable.

In addition, an architecture is required that offers a single access point to internal/external data. Onboarding data to the "access layer" follows a strict governance: Minimum standards on dataset definitions, data cataloguing, as well as ownership and stewardship are required at Allianz Global Investors. While in the past data ownership was mainly directed to the own consumption (e.g., products data for the products function), the main task for owners now is to ensure adequate usage outside their function. Like oil, raw data is not valuable in itself: Value creation happens by connecting high-quality, well-understood, governed datasets, and by 'refining' into fuel that can power the business.

A Typical Use Case in Portfolio Decision Making Processes

At Allianz Global Investors, investments, data, and technology are the drivers of Data Democratization: For decision support systems, both systematic and fundamental research information are combined (e.g., portfolio holdings with third-party credit rating or ESG scores). In turn, the generated signaling data is stored back to the access layer to allow cross-asset-class reuse. Now, Data Democratization does not only allow better and deeper data analytics for individual users but also drives cross-functional collaboration. Hence, data truly becomes a driver for business success.

Research Report

Jump on the Hype – German Retail Investors and the Gamestop Frenzy

GAMESTOP, A COMPANY THAT WAS PRESUMED DEAD DUE TO SHRINKING PROFITS OF ITS BRICK-AND-MORTAR BUSINESS MODEL, HIT THE HEADLINES BECAUSE OF A SHORT SQUEEZE OF ITS STOCK PRICE. THE POPULAR OPINION REPORTED BY MAINSTREAM MEDIA SUGGESTED THAT THE GAMESTOP FRENZY WAS EXCLUSIVE TO YOUNG AND INEXPERIENCED INVESTORS GATHERING ON THE SOCIAL MEDIA PLATFORM REDDIT. IN CONTRAST, OUR RESULTS INDICATE THAT ALSO MORE EXPERIENCED RETAIL INVESTORS IN GERMANY PARTICIPATED.

Andrej Artuschenko
Fabian Nemeczek
Daniel Weiss

Introduction

In just a few days, the Gamestop (GME) stock price rose nearly 900 times from its record low, reaching an interim high of about USD 480 (EUR 405) on January 28th, 2021. The implied market cap of over USD 27 million made GME temporarily more valuable than many companies listed in the S&P 500.

The mainstream media depicted this development as a result of young and inexperienced small investors pooling their financial resources to sabotage hedge funds' short positions in shares of ailing companies. The events surrounding the GME short squeeze have also captivated audiences in Germany, including both laypeople and financial market experts. Contrary to the well-known Volkswagen short squeeze in 2008, the recent turmoil around GME was mainly driven by retail investors.

This report provides a brief overview of the recent events, and documents the reaction of German retail investors to the Gamestop hype.

The Story of the Gamestop Frenzy

While it is not easy to identify a clear starting point, the recent GME hype is traced back to a video by Keith Gill, a famous Youtuber, posted in summer 2020. In his video, he analyzed the GME stock and presented it as undervalued and emphasized that the short interest was over 100% of the outstanding shares, which was a stark contrast to the average short position of 5% back then (Angel, 2021). Like many other such polarizing analyses, this video gained attention on the popular Reddit message board, WallStreet Bets. Its community is known for its own unique culture and terminology, popularizing terms such as meme-stocks. The latter are characterized by high volatility and prominence among younger investors. Most importantly, they have a strong Social Media presence and tend to be overvalued due to the fear of missing out (FOMO) phenomenon (Semenova and Winkler, 2021).

Motivated by the initial analysis of Keith Gill, the GME investment case was carried over to other discarded companies like AMC, Nokia, Blackberry, and highly speculative stocks, such as Rocket Company, Etsy, and Palantir. In particular, these stocks attracted the interest of the Reddit community because – similar to GME – their short interest was higher or close to 100%. This exaggeration on the part of the short-sellers led to the resentment of hedge funds and their role in the financial system.

Figure 1 shows the daily closing prices of the GME stock between December 1st, 2020, and March 1st, 2021. The catalyst of the turnaround speculation was the announcement of Ryan Cohen as a new board member on January 11th. This made GME the most discussed stock on Reddit, illustrated by the increase in Reddit posts mentioning "GME" afterwards. The posts rumoured that Cohen was planning to transform GME into an e-commerce platform. The first substantial price increase of 68% on January 13th sparked the attention of the public and resulted in the first reports in the mainstream media, as indicated by the increase in Google Trends on GME.

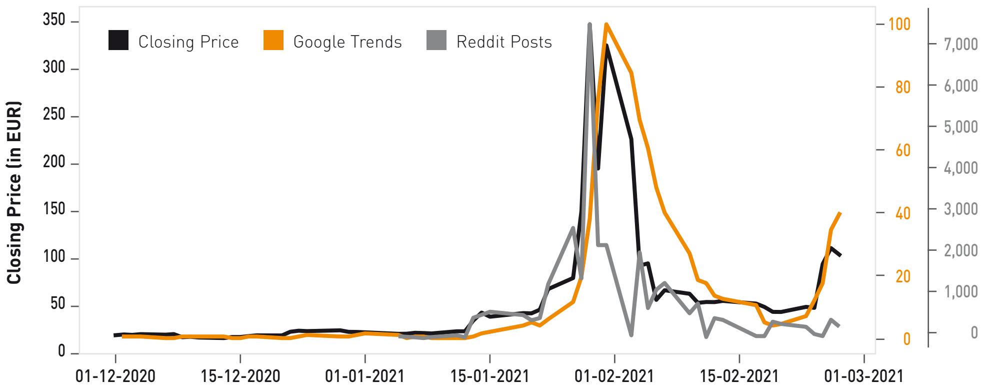

Figure 1: Daily Closing Prices of GME, Google Trends, and Reddit Posts during the Gamestop Frenzy

Note: Reddit posts show how often "GME" was mentioned per day on the Reddit message board WallStreetBets; Google Trends represent a normalized measure of Google searches for "Gamestop" and "GME", ranging from 0 to 100 where 100 indicates the mostly searched term.

Triggered by emerging bandwagon effects and FOMO, more and more investors participated in the Gamestop frenzy. In the following weeks, the price of GME and other meme-stocks increased further, forcing short-selling hedge funds to cover their positions. In the case of GME, the resulting short squeeze led to a multiplication of the stock price (intraday) to over USD 480 (EUR 405). In turn, the Malvin Capital hedge fund, the biggest opponent of GME, lost 30% of its value. In fact, Malvin had to raise an interim sum of USD 2.75 billion in emergency funds before closing all their positions on January 26th. In the meantime, the hedge fund Citron also closed all its positions with a 100% loss (Chohan, 2021).

An additional controversy arose when on January 28th, neo-brokers, such as Robinhood in the US or Trade Republic in Germany, imposed trade restrictions on meme-stocks, which led to substantial price declines on the same day. Interestingly, as shown by the slightly delayed peak in Google Trends, the mainstream media's attention peaked only days after GME reached its all-time high on January 28th.

A few days after the trade restrictions were lifted again, the US House Financial Services Committee held a hearing to recapitulate the trading hype and the controversial trade restrictions, with no significant results so far.

Overall, the mainstream media framed the story as a David versus Goliath battle of young and inexperienced retail investors against hedge funds. Even though the public drew analogies to Volkswagen in 2008, there is a crucial difference: while a takeover attempt by Porsche initiated the Volkswagen short squeeze, the Gamestop frenzy arose through Social Media coordination among retail investors.

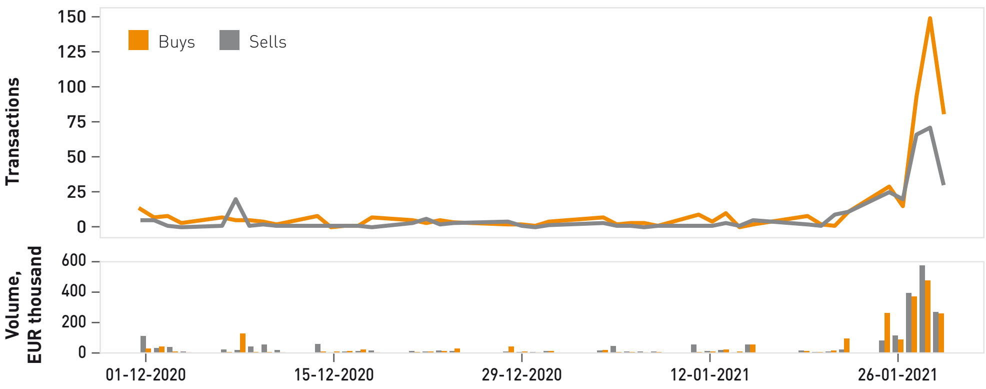

Figure 2: Daily Transactions and Trading Volume of Meme-stocks Traded By Private Investors of a German Retail Bank

Note: We pooled together all meme-stocks (i.e,. Gamestop, AMC, Nokia, Blackberry, Rocket Company, Etsy, and Palantir).

Data

We obtain data from a German bank with a broad offering in retail banking services. The bank provides trading data, including customer demographics and administrative records of individual customers. Our selected sample comprises a six-digit number of customers and ranges from December 1st, 2020, until January 31st, 2021. This encompasses the most critical period of the Gamestop frenzy. Focusing on meme-stock traders only, we identified about 300 customers who we take a closer look at in the following.

The Reaction of German Retail Investors

Out of these customers, we see that about 80% are male and on average 46 years old. About 55% are employees while self- and unemployed, students, and retirees are represented with roughly 5% each and others with the remaining 25%. Moreover, on average, the investors have been the bank's customer for 15 years, trade about four times per month and have average monthly transaction volumes of about EUR 29,000.

In Figure 2, daily transactions and volumes are depicted. Overall, we see that the number of buys and sells as well as the daily transaction volume surge in the last week of January 2021. Specifically, we observe 380 buys and 220 sells. Interestingly, the actual transaction volume of EUR 1.6 million of sells exceeds the buy volumes of EUR 1.5 million.

In sum, we identified 83 completed transactions that were bought and subsequently sold during the Gamestop frenzy. On average, the realized returns amount to around 15.0%. Furthermore, by focusing on the last observed trading week, we do not notice any heterogeneity in different characteristics such as age, gender, or employment status.

Conclusion

Overall, our results illustrate that participation in the Gamestop frenzy was more widespread as portrayed in the mainstream media. In fact, our investor data shows that also more experienced traders with relatively larger portfolios participated. This shows that the media's reporting was rather polarizing in putting the young and inexperienced investors exclusively into the spotlight.

References

Angel, J. J.:
Gamestonk: What Happened and What to Do about It.
In: SSRN Electronic Journal, 2021.

Chohan, U. W.:
Counter-Hegemonic Finance: The Gamestop Short Squeeze.
In: SSRN Electronic Journal, 2021.

Semenova, V.; Winkler, J:
Reddit's Self-Organized Bull Runs.
In: INET Oxford, Working Paper No. 2021-04.

Research Report

Phish Me If You Can: Insights from an Eye-Tracking Experiment

PHISHING E-MAILS CONTINUE TO POSE A TOP THREAT TO AN ORGANIZATION'S INFORMATION SECURITY. DESPITE TECHNICAL ADVANCES, THE BURDEN OF DETECTING AND DEALING WITH THEM ULTIMATELY REMAINS ON THE SHOULDERS OF THE INDIVIDUAL EMPLOYEE. THIS ARTICLE PRESENTS RESULTS OF A MULTI-METHOD PHISHING EXPERIMENT INCLUDING THE USE OF AN EYE-TRACKING DEVICE TO ASSESS EMPLOYEES' ACTUAL AWARENESS OF PHISHING AND INFLUENCING FACTORS. PRACTICAL IMPLICATIONS FOR SECURITY TRAININGS ARE ALSO DISCUSSED.

Lennart Jaeger Andreas Eckhardt

Introduction

Information is central to the functioning of modern organizations and the most important factor holding organizations together. This centrality ultimately gives information critical value, and safeguarding information has become a top management priority in many organizations. Yet, as a consequence of an increasingly connected world and the strong dependence on information systems, organizations are continually finding it difficult to keep their information assets secure. Many notorious security incidents in the recent past show that security attacks from outside the organization as well as employees' misbehavior inside the organization can have grave consequences, including corporate liability, loss of reputation, and financial damage. To ensure information security, organizations have often relied only on technology-based solutions in the past, such as antivirus software, firewall management systems, or intrusion detection systems. But the sole reliance on these types of solutions is not sufficient because it is estimated that 47-60% of all security incidents are either directly or indirectly due to employee misconduct (Verizon, 2020).

As the focus of information security continues to shift towards individual and organizational perspectives, organizations realize that employees, often considered as the 'weakest link' in the information security chain, can also be vital assets to reduce security risks. Because individuals who are aware of their organization's security mission and ideally committed to it are the key to strengthening information security, understanding *information security awareness* (hereinafter: ISA) is vital for organizations that want to leverage their human capital (Bulgurcu et al., 2010). Accordingly, in realizing the dual role of their employees, as both allies and sources of security threats, organizations have started to invest in security education, training, and awareness programs to ensure that their employees have an appropriate level of knowledge about information security along with an appropriate sense of responsibility. However, the unabated prevalence of information security incidents due to employees' intentional or unintentional actions shows that reality still falls short of this ideal.

In phishing, for example, the burden of detecting and coping with phishing mails ultimately remains on the shoulders of the individual employee. Questions about why phishing works are fundamentally questions about awareness: When individuals fall for a phishing mail, did they deliberately assess the situation (e.g., check sender address) or did they click on it without much deliberate thought (Dennis and Minas, 2018)? To answer this question, studies have mainly investigated the impact of E-mail recipients' characteristics, and the characteristics of the E-mail itself. However, research has largely overlooked interactions between the recipient of a phishing mail and the situation the recipient is in, i.e., the moment when an individual processes an E-mail.

Thus, since the full extent of individuals' actual awareness in a security-related situation remains to be clarified, we introduce the concept of *situational* ISA as individuals' knowledge of particular security threats transported by security-related information cues captured in a situational process in the immediate system environment. Our research aims to empirically examine determinants and consequences of individuals' situational ISA.

Phishing Eye-Tracking Experiment

We conducted an experimental study in the context of E-mail communication, in which participants received a mailbox exercise. Participants took the role of an employee in a fictitious organization and read and processed 20 E-mails, including six phishing mails, stored in a webmail inbox. The phishing mails varied in contextual relevance (i.e., the alignment with recipients' work responsibilities) and misplaced salience (i.e., salient design features including colored text, logos, buttons, and pictures). The experiment was conducted with 107 employees from various organizations. 55% of them were men and the average participant was 40 years in age, used a computer at work for 6.6 hours per day, and had 3.4 E-mail accounts.

An eye-tracking device was used to record participants' eye movements to security cues (e.g., sender address, real URL link, file info of attachment, etc.). Situational ISA was measured by the number of security cues that individuals paid attention to compared to all available security cues. In other words, the more they looked at, the better. As visualization, Figure 1 provides an example of someone with a high degree (left) and of someone with a low degree of situational ISA (right). Blue dots and lines are the areas participants looked at. Differently colored squares represent the security cues. Security-related behavior was measured by coding protective actions taken during the experiment including whether participants deleted/archived the phishing mail or notified the helpdesk, whereas clicking on a phishing link or downloading an attachment was considered as unsafe behavior. After participants processed the 20 E-mails, they filled out a questionnaire to capture other variables of interest for the study.

Empirical Findings

We found that, in 26% of all cases, participants clicked on the enclosed links or downloaded the attachment in the phishing mails. This result is in line with industry experiences and phishing benchmarking studies (KnowBe4, 2018). Furthermore, in a quarter of those cases, login data was submitted or the attachment opened. On the other hand, in 38% of all cases, participants deleted the phishing mail or archived it in the spam folder, while in only 8% of all cases participants reported the phishing mail to the IT helpdesk. To explain such security-related behaviors, we developed and empirically tested a model of situational ISA (see Figure 2) by drawing on prior research of situation awareness, phishing literature, and protection motivation theory as applied in information security (Boss et al., 2015). We integrate key factors which draw on the interaction between the individual employees and their system environment in achieving situational ISA.

At the individual level, prior experience with phishing positively influences situational ISA (*H1*). Experienced individuals demonstrate their awareness by attending to more security cues. This suggests that experience enables the development of schemata and recognizing the critical cues that activate pattern matching of the phishing mail with schemata in the process of forming awareness.

Contrary to what we expected, the personality trait of agreeableness did not significantly impact situational ISA (*H2*). Although agreeable individuals tend to be more trustworthy and susceptible to phishing, in our case, it did not lead to paying less attention to security cues. However, agreeable individuals could still fall for a phishing mail by being influenced by compelling parts of the E-mail text rather than security cues.

At the system level, situational ISA is negatively influenced by contextual relevance (*H3*) and misplaced salience (*H4*). When the premise of a phishing mail is aligned to their work context, individuals pay attention to fewer information security-related cues in phishing messages. Moreover, when phishing mails have salient design elements, such as logos, images, or buttons, they direct attention more

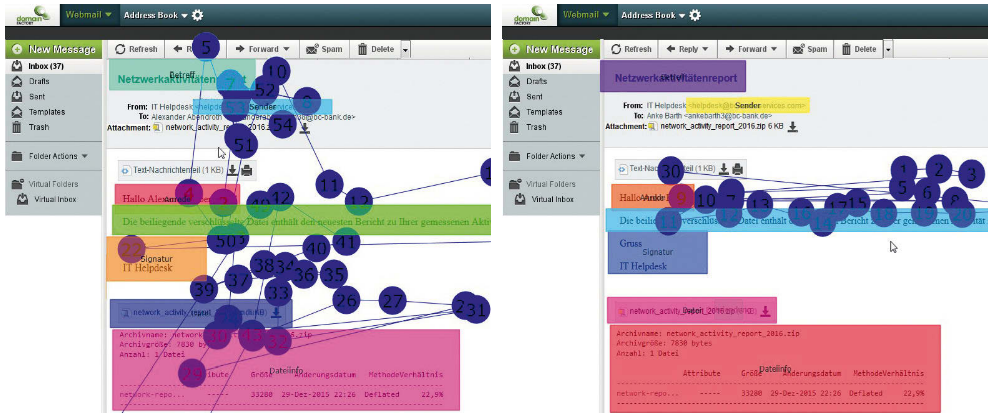

Figure 1: Gaze Plot Comparison (adapted from Jaeger and Eckhardt, 2020)

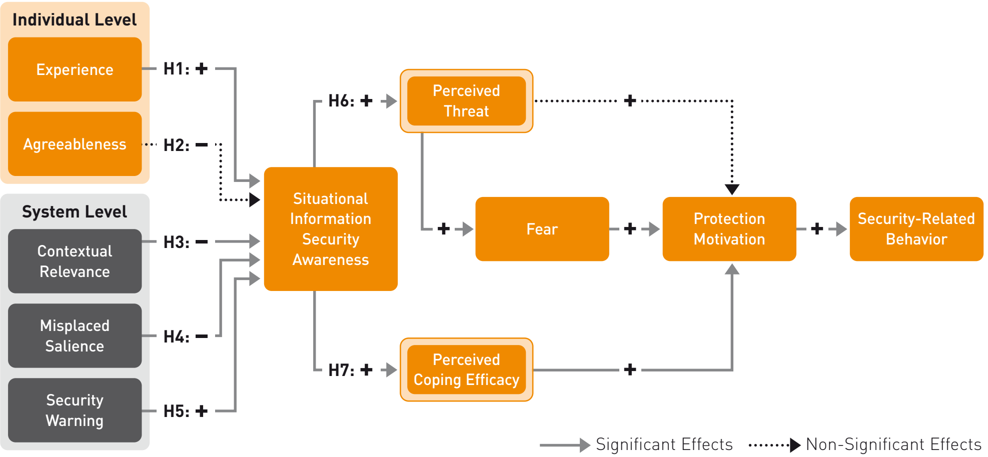

Figure 2: Research Model of Situational Information Security Awareness

away from security cues than E-mails with just plain text.

Moreover, a security warning raises individual's situational ISA (*H5*). Participants who received a security warning during the experiment attended to more security cues. This indicates that warnings can serve as a critical cue to activate the mechanisms of matching the pattern of a phishing mail with existing schemata.

Regarding the consequences of situational ISA, we find that it influences both the development of threat and coping appraisals. Situational ISA is a significant determinant for perceived threat (*H6*). Since security cues, like the file extension of an attachment (e.g., .exe), may indicate whether opening such attachments may lead to the corruption of data, examining such cues provides an informational basis to evaluate how threatening an E-Mail is.

Additionally, while there was no direct influence of perceived threat on protection motivation, we find an indirect influence through individual's fear of phishing. In other words, when individuals see phishing as threatening, the fear of phishing is generated as an outcome, which also raises their motivation to take protective actions against phishing, termed protection motivation.

Regarding coping appraisal, we find that individuals who paid attention to more security cues, also feel more confident to take relevant actions and perceive that these actions are effective, taken together termed perceived coping efficacy (*H7*). This also raises their protection motivation. Protection motivation ultimately increases security-related behaviors, such as deleting the phishing mail or notifying the helpdesk.

Implications for Practitioners

Our findings have important practical implications for information security management. Individuals with phishing experience pay attention to more security cues, such as sender address or real URL links. This indicates that their mental models of phishing are more complex and contain more links between concepts related to the characteristics of phishing attacks than those with less phishing experience. Accordingly, training programs should be designed to provide information about the interconnectedness of security cues; for example, how an unknown sender may be connected with an impersonal greeting, which could be related to a malicious attachment or fake link.

The negative impact of a phishing mail's contextual relevance on situational ISA emphasizes the importance of varying phishing exercises suitably and challenge employees with contextually relevant E-mails to provide training on new scams. Training implementers must understand the relevancy of a phishing mail for their trainees. For example, certain work groups may have to regularly interact with external third parties and may be more exposed, which could make them more susceptible to phishing. On the other hand, they could actually be the ones that acquire situational ISA more easily. This is due to the fact that they have to regularly match patterns of E-mails with their mental library of what an E-mail should look like to determine whether it is a legitimate or phish.

To manage different abilities, the used training set of phishing mails should differ in their detection difficulty by varying the number of security cues that are manipulated (e.g., is only the sender address and link fake, or also other parts in the message). More experienced or frequently exposed work groups may benefit from a variation of more difficult phishing mails that update and enhance their mental models of phishing and counter possible stereotypes that may develop by being repeatedly exposed to similar phishing mails. Conversely, less experienced or exposed work groups may respond more favorably to more simple phishing mails with fewer cues being manipulated to initially help them develop a mental library of prototypical phishing mails.

References

Boss, S. R.; Galletta, D. F.; Lowry, P. B.; Moody, G. D.; Polak, P.:
What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors.
In: MIS Quarterly, 39 (2015) 4, pp. 837–864.

Bulgurcu, B.; Cavusoglu, H.; Benbasat, I.:
Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.
In: MIS Quarterly, 34 (2010) 3, pp. 523–548.

Dennis, A. R.; Minas, R. K.:
Security on Autopilot: Why Current Security Theories Hijack our Thinking and Lead Us Astray.
In: ACM SIGMIS Database, 49 (2018) 1, pp. 15–38.

Jaeger, L.; Eckhardt, A.:
Eyes Wide Open: The Role of Situational Information Security Awareness for Security-Related Behaviour.
In: Information Systems Journal, 31 (2021) 3, pp. 429-472.

KnowBe4:
Report 2018: Phishing by Industry Benchmarking, https://info.knowbe4.com/2018-phishing-by-industry-benchmarking-report, 2018.

Verizon:
2020 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir, 2020.

Insideview

Is Platform Lending Just a Flash in the Pan?

INTERVIEW WITH STEFAN FENNER

Dr. Stefan Fenner
Managing Director
CAPVERIANT GmbH

Lending platforms are on the rise. Even though the platform-idea is not new, they finally seem to make their way within the last two years. Why now?

First of all, the most critical hurdle for a platform is to be on the market in the second the client behavior is ready for a change to a digital solution. While exactly hitting this point seems almost impossible, staying power paired with an absolutely deep conviction is the key to success. We see b2b digitization moving much faster right now, driven by the pandemic, but also a deeper trust transferred from positive digital b2c experiences that is bringing more traction to lending platforms in Germany.

Is that move to platforms sustainable or just a flash in the pan?

I am convinced the high level of standardization on the one hand and fragmentation on the other hand provide the basis for public-sector lending platforms to be successful. Current environment works as an accelerator and enables the playing field to convince clients that platform lending is beneficial for all participants in the value chain and that's the trigger we have been waiting for. I believe, we will see some fast developments within the next 12 months in most lending segments.

Do you also see a wave of consolidation coming up?

As platform markets are in some respects often a "winner takes it all" model, I think we will see various consolidations within the next 12-18 months. Looking at consolidation, ownership structure is a central trigger. FinTechs that are backed by venture capital and are not in a dominant position, will eventually face trouble in their next financing rounds as market maturity is, at least in some segments, in a later stage now. This will definitely support a more sophisticated trend towards consolidation.

Public-sector financing is not known for being fancy or even digital – why do you believe it will be among the winners in platform lending?

First of all, a good platform can be fancy, but fanciness alone does not win the game. The most important thing is to address the clients' problem with a suitable digital solution. And platforms usually have two client groups whose key demands are often different: For borrowers, full market overview, best price, and a digital processing are the main drivers to move to a platform. For lenders, the best available price on the borrower side can affect the margin. So, the offer for a platform lender is the volume increase through a digital access to new clients as well as the digital process itself. At Capveriant, we see public-sector financing today as a highly intransparent and very fragmented market on lenders and even more on borrowers' side. Nevertheless, the product from a financing point of view is very plain vanilla and the volume per trade is relatively high, what makes it a perfect platform business from our point of view. As we see at least four platforms in our segment, we are very convinced that public-sector financing will move even faster to a platform like Capveriant.

Are lending platforms going to disrupt bank lending fully in long term?

The developments we have seen so far and the ones we are expecting do not look like disruption today. But as client behavior is changing and substantial volumes are moving to platforms, banks should think about how they can benefit. We as a platform are delivering digitalized processes and an easy access to new client segments directly to the door sill. All banks have to do is sign in.

Thank you for this interesting conversation.

Infopool

News

Best Paper Award 2020 of the "Journal of the Association for Information Systems"
The authors Jens Lausen, Benjamin Clapham, Michael Siering, and Peter Gomber have won the 2020 Best Paper Award of the renowned "Journal of the Association for Information Systems" (JAIS) for their publication "Who Is the Next "Wolf of Wall Street"? Detection of Financial Intermediary Misconduct". Congratulations!

EHI Science Award 2021
Dr. Christoph Brenner received the Science Award 2021 of the EHI Retail Institute for his dissertation "Innovations in Performance Marketing". The dissertation was supervised by Prof. Hinz. Congratulations!

Prof. Skiera Designated as One of the Most Productive Researchers in Marketing
The American Marketing Association (AMA) lists Bernd Skiera in their 2020 worldwide ranking of the most productive researchers in marketing during the last ten years on Rank 20 (for AMA journals) and Rank 42 (for Premier Marketing Journals). In their global ranking, the AMA considers authors according to the number of publications in the Journal of Marketing and the Journal of Marketing Research. Congratulations!

Successful Disputation
Konstantin Bräuer successfully defended his dissertation titled "Essays in Household Finance". In his dissertation, Konstantin studies empirically the financial choices of retail investors, in particular, whether investor psychology can explain heterogeneity in observed investment choices, how financial technology affects investment choices, and to what extent investment choices are linked to consumption behavior. The dissertation was supervised by Prof. Hackethal. Congratulations!

Dr. Alves Werb Accepted Position as Tenured Professor
Dr. Gabriela Alves Werb, former doctoral student of Prof. Skiera, accepted an offer as a tenured professor of Business Information Systems at the Faculty of Computer Science and Engineering at Frankfurt University of Applied Sciences. She has joined the Informatics Cluster at the Faculty of Computer Science and Engineering in the 2021 summer term with lectures in the Business Information Systems degree programs.

Data Management Lab is Part of the New National High Performance Computing Network
In the future, the Data Management Lab of TU Darmstadt will be a member of the National High Performance Computing (NHR) network funded by the federal and state governments. In its meeting on November 13, 2020, the Joint Science Conference (GWK) decided to admit TU Darmstadt together with RWTH Aachen University to the consortium.

For a comprehensive list of all efl news postings and efl publications see: *https://www.eflab.de*

Selected efl Publications

Bender, M.; Panz, S.:
A General Framework for the Identification and Categorization of Risks: An Application to the Context of Financial Markets.
In: Journal of Risk, 23 (2021) 4, pp. 21–49.

Bucher-Koenen, T.; Hackethal, A.; Koenen, J.; Laudenbach, C.:
Gender Differences in Financial Advice.
In: 48th Annual Meeting of the European Finance Association (EFA); Milan, Italy, 2021.

Frank, M.:
Combatting the Neutralization of Security Policy Violations: Insights from the Healthcare Sector.
In: Proceedings of the 29th European Conference on Information Systems; Marrakesh, Morocco, 2021.

Kalda, A.; Loos, B.; Previtero, A.; Hackethal, A.:
Smart(Phone) Investing? A within Investor-Time Analysis of New Technologies and Trading Behavior.
In: 48th Annual Meeting of the European Finance Association (EFA); Milan, Italy, 2021.

Keller, K.; Schlereth, C.; Hinz, O.:
Sample-based Longitudinal Discrete Choice Experiments: Preferences for Electric Vehicles over Time.
In: Journal of the Academy of Marketing Science, 49 (2021) 3, pp. 482–500.

Wieringa, J.E.; Kannan, P.K.; Ma, X.; Reutterer, T.; Risselada, H.; Skiera, B.:
Data Analytics in a Privacy-Concerned World.
In: Journal of Business Research, 122 (2021), pp. 915–925.

ANNUAL CONFERENCE 2021

The efl cordially invites you to its Annual Conference 2021 on "Data, Liquidity & Market Structure – What's next for Europe?". The event will take place on September 30, 2021, and is organized by Prof. Gomber and his team. In order to ensure predictability and the safety of all participants, the Annual Conference 2021 will be online (start at 3 pm). Participants will gain insights from leading researchers, practitioners, and regulators on the role of data and data consolidation in European financial markets, the upcoming regulatory changes due to the MiFID II / MiFIR review, and the implications of increased retail trading volumes against the background of neobrokers and payment-for-order-flow.

The registration form and further information are available on our conference website: **https://www.eflab.de/annual-conference-2021**. As always, the participation is free of charge.

Infopool

RESEARCH PAPER: PREDICTING LABOR MARKET COMPETITION: LEVERAGING INTERFIRM NETWORK AND EMPLOYEE SKILLS

Firms compete for consumers in the product market – but also for employees in the labor market. Well-known examples of such labor-market competition include Walmart and Amazon, or Tesla and Apple. Identifying labor-market competitors is, however, challenging, because such competition often spans across different industries.

This article proposes to identify labor-market competitors based on profile data from LinkedIn. By tracking employees' job history across firms over time, the authors construct a network of human capital flow. The use case of this network is two-fold: First, it allows to predict future employee migration to competitors. Second, it allows to identify potential future product-market competitors (e.g., Apple hiring from Tesla in a possible attempt to produce a competing car).

Liu, Y.; Pant, G.; Sheng, O. R.
In: Information Systems Research, 31 (2020) 4, pp. 1443–1466.

RESEARCH PAPER: ONLINE TO OFFLINE: THE IMPACT OF SOCIAL MEDIA ON OFFLINE SALES IN THE AUTOMOBILE INDUSTRY

Based on the various research streams regarding multi-channel marketing, the authors examine the effectiveness of Social Media advertising on offline sales by differentiating between firm-generated and user-generated content. Using a panel vector autoregressive model, the study shows that firm-generated content is more effective in generating offline sales than user-generated content. In addition, firm-generated content has both a higher long-term effect and it takes shorter time to become effective. However, the content of firm-generated content does not have an impact on offline sales. Only the volume of firm-generated content effects the purchase decisions of customers. Based on these findings, managers can adjust their Social Media marketing to boost offline sales.

Wang, Y.-Y; Guo, C.; Susarla, A.; Sambamurthy, V.
Forthcoming in: Information Systems Research (2021), pp. 1–17.

efl insights

The efl publishes the insights in the form of a periodic newsletter which appears two times a year. Besides a number of printed copies, the efl insights is distributed digitally via E-mail for reasons of saving natural resources. The main purpose of the efl insights is to provide latest efl research results to our audience. Therefore, the main part is the description of two research results on a managerial level – complemented by an editorial, an interview, and some short news.

For receiving our efl insights regularly via E-mail, please subscribe on our homepage www.eflab.de (> NEWS > SIGN UP EFL INSIGHTS) as we need your E-mail address for sending the efl insights to you. Alternatively, you can mail your business card with the note "efl insights" to the subsequent postal address or send us an E-mail.

Prof. Dr. Peter Gomber
Vice Chairman of the efl – the Data Science Institute
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
D-60629 Frankfurt am Main

insights@eflab.de

Further information about the efl is available at
www.eflab.de.

House of Finance

The efl – the Data Science Institute is a proud member of the House of Finance of Goethe University, Frankfurt.
For more information about the House of Finance, please visit www.hof.uni-frankfurt.de.

For further information please contact:

Prof. Dr. Peter Gomber
Vice Chairman of the
efl – the Data Science Institute
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
D-60629 Frankfurt am Main

Phone +49 (0)69 / 798 - 346 82
E-mail gomber@wiwi.uni-frankfurt.de

Press contact
Phone +49 (0)69 / 798 - 346 82
E-mail presse@eflab.de

or visit our website
http://www.eflab.de