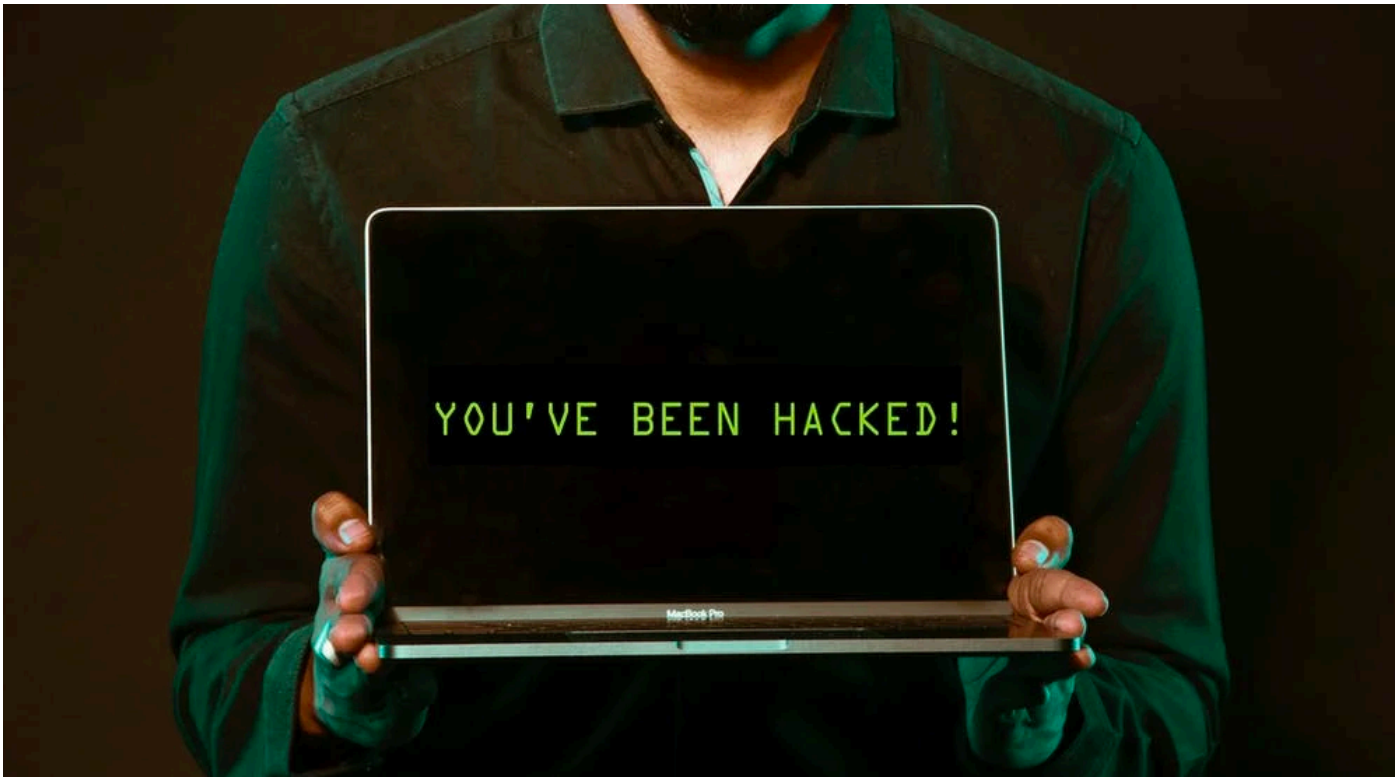
Fraud Detection and Prevention



Algorithmic Trading

Algorithmic trading is a process of executing orders using automated pre-programmed trading instructions that are constantly evaluating variables such as price, volume, and time. This major advantage algorithmic trading is its ability to leverage the superhuman speed and superior processing resources of computers compared to the limitations of human traders.

There are many common types of algorithmic trading and some powerful tools in Python for coding and executing these techniques that you will be learning about later in this bootcamp.

Customer Service and Recommendation

With the rapid rise of subscription-based SaaS programs and services available both on the Internet and via other streaming sources, in tandem with the emergence of highly-competitive global marketplaces, customer

churn (i.e. when you will lose a customer) has become a major focus of a variety of businesses across a broad spectrum of business sectors.

Unknowingly, most organizations have the data they need at their fingertips to accurately predict when this is happening and perhaps more importantly, why this is happening and how that knowledge can be used to improve customer service, customer retention, and to make better recommendations (e.g. curation) to their existing clients.

As an example of this type of service, Netflix held an open competition for the public called the **Netflix Prize** to create a better recommendation engine and curation algorithm for its customers. The grand prize of $1,000,000 was awarded to the BellKor's Pragmatic Chaos team which improved Netflix's own algorithm for predicting user's ratings of movies by 10.06%. The $1,000,000 was considered a very small reward when viewed in the perspective of the long-term value this improvement will provide to Netflix's bottom line.

Risk Management in Banks and Financial Institutions

Machine learning allows AI systems to reveal insights within extremely large

and diverse data sets. This capability has obvious applications for banking risk management, and when implemented, can lower operational and compliance costs while providing decision-makers with more accurate credit scores than previously possible.

Some common ways AI can be used to help enable better risk management:

1. **Near real-time fraud detection** with more and more shopping going online due to COVID and other factors, the available landscape for fraudulent actors online has grown as well. The ability to have unsupervised learning models that identify patterns on their own without being dependent on historical data allow banks exponentially more techniques and tools for identifying fraud than prior techniques that were based more on physical or in-person transactions.
2. **Securely storing and sharing KYC information** KYC (Know Your Client) when verified and stored in a way were banks can share this valuable client data, can greatly streamline the loan approval process and make it much easier to rapidly identify missing, fraudulent, or stolen information.
3. **Improving regulatory and compliance activities** Compliance and risk management are closely aligned, as compliance with federal and global regulations helps protect banks from a variety of unique risks. The process of compliance is expensive, though, costing the banking industry $270 billion a year and accounting for 10 percent of operational spending.

   This is an important improvement. Machine learning is vastly superior to human beings for this task because not only can ML-powered programs process massive amounts of data in rapid time while analyzing countless variables, but they can also identify important correlations that would never stand out to us. JPMorgan Chase is a great example of this. The bank previously employed a whole team of lawyers and loan officers to spend 360,000 hours each year tackling mundane tasks,

including reviewing commercial-loan agreements. But by using an ML-powered program, COIN, the bank was able to process 12,000 credit agreements in several seconds. This not only shortened the time required to review documents, it also decreased the number of loan-service mistakes. JPMorgan Chase is now planning to deploy machine learning in more complex areas, such as credit default swaps and custody agreements..

Network Security

Artificial Intelligence (AI) can prove to be the method of choice when battling against cyber-attacks. In recent years, the attacks on tech companies and financial institutions have proved to be a big issue when it comes to network security. Government agencies and companies like Oracle, US Department of Justice, US Democratic National Committee (DNC), the Internal Revenue Service (IRS), LinkedIn and Snapchat have all been defenseless against such attacks.

AI plays a major role against cyber-attacks using anomalous patterns in data that can be easily detected and interpreted as threat more efficiently than any human can. Giants in the tech industry like Microsoft, IBM and Amazon, to name a few, are heavily vested in AI to prevent any sort of cyber-attack. The data used for this methodology is data from the previous attacks and patterns, including any information related to the malware and cyber-attack are also helpful in the AI design.

Such algorithms used include: XGBoost and Neural Networks. Microsoft has launched a malware detection challenge using machine learning on Kaggle. You can read more about one the solutions on GitHub.