AI and Its Impact on Cybersecurity

Part 5: How Algorithms Decide What You See and Pay!

In Part 4, we saw how search engines evolved from counting keywords to understanding what you really mean. But search results aren't the only thing being decided for you online. Right now, algorithms are deciding what posts you see on social media, what shows Netflix recommends, and which ads follow you around the internet. And here is the surprising part, algorithms sometimes even decide how much you pay for things. Welcome to Part 5, where we explore the algorithms that shape your entire online experience, often in ways you never notice.

The Humble Algorithm

We've mentioned algorithms throughout this series, and in Part 4 we even introduced you to Al-Khwarizmi, the Persian mathematician from 780-850 AD whose work gave algorithms their name. Algorithms have been around for thousands of years. Archaeologists have found step-by-step mathematical procedures on Sumerian clay tablets dating back to 2500 BC! But simply put, an algorithm is just a recipe: a concrete, step-by-step procedure for solving a problem. The difference between those ancient algorithms and today's AI-powered algorithms is like the difference between a handwritten recipe card and a smart oven that adjusts cooking time based on what you're making. In this part, we'll look at the algorithms you interact with every day and how they've evolved from simple rules into AI systems that predict your preferences, influence your choices, and yes, sometimes even change prices based on your behavior. This is the last time we'll look under the hood of how AI works before we shift our focus to how it's being used by bad actors trying to do more than just get you to watch a video or pay more for something. They are trying to steal from you!

Social Media Algorithms

Do you remember way back in 2004 when your Facebook feed (known back then as "TheFacebook"!) just showed posts from friends in chronological order? The most recent post appeared at the top, then the next most recent, and so on. It was easy to find a post; you just scrolled back far enough to the date it was posted. Those days are long gone. Today's social media feeds are controlled by AI algorithms that decide what you see, when you see it, and in what order. These algorithms don't follow simple rules, they're predicting what will keep you engaged based on patterns in your behavior. So what exactly are these algorithms looking at? Everything!

Think back to the paper written by Google computer scientists called Attention is All You Need. That paper suggested that if an LLM could focus on all the data presented at once, it could understand better, have better context and then provide more accurate responses.

Social media algorithms pay attention to everything as you are engaging with posts. Here's what these algorithms are paying attention to.

1. **What you like**: This is not just about clicking the "Like" button or "Thumbs Up" icon, the algorithm determines what you like by how long you stay on that post, if you click to see more, or if you watch a video all the way through.
2. **What you comment on**: The algorithm learns what interests you by what comments you make.
3. **What you share**: If you share a post, the algorithm will weight this heavily because it sees you as being very interested in that topic.
4. **What you click**: You teach the algorithm by what you click. If you click a link in a post, click on the profile or open a photo or video, this tells the algorithm that you are interested in that person, that post or that photo or video.
5. **What you don't like**: Algorithms also learn what you don't like by what you pass by. If you scroll right past a post on underwater basket weaving, the algorithm puts that into its memory bank as something you really couldn't care less about.

This is the pattern recognition that we discussed back in part 2. The algorithm is analyzing millions of data points all in a fraction of a second to determine what comes next in your feed.

Why This Matters: Different Feeds for Different Folks

Why do algorithms function this way? Two reasons: Engagement and money. But the first drives the second and it always comes down to money. Social media platforms make money from advertising. Advertisers pay more when users spend more time on the platform clicking, scrolling, and viewing ads. The algorithm's job is simple: keep you engaged as long as possible. If showing funny cat videos keeps you scrolling for 30 minutes, but political news makes you close the app after 5 minutes, guess what you'll see more of? Cat videos.

This wasn't always the business model. When Facebook launched in 2004, it was an instant hit with users, but investors weren't sure how it would make money. It took seven years for Facebook to figure out sustainable advertising revenue. Once they did, the focus shifted from just connecting people to keeping people on the platform as long as possible. That's when the algorithmic feed was born.

And here's the kicker: your feed looks completely different from your friend's feed, even if you follow all the same people and pages. The algorithm is predicting what will keep *you* engaged, not what's actually most recent or most important. You might see posts from certain friends every day while posts from others never appear, even though you're connected to both. That's not random—that's the algorithm deciding what keeps you scrolling.

This series isn't about judging whether algorithms are good or bad, but it's worth noting that they can create an "ideal world" that isn't actually ideal. If all you see is what you like, you could miss out on other important issues or perspectives. Over time, your feed becomes increasingly tailored to your existing interests and beliefs. This creates what's called a "filter bubble" or "echo chamber." You end up seeing a curated version of the world, not the whole picture. Just something to be aware of.

Recommendation Engines

Social media feeds aren't the only place algorithms predict what you'll like. Every time you open Netflix, YouTube, Spotify, or Amazon, recommendation algorithms are analyzing your behavior to predict what will keep you engaged.

Have you ever wondered how Netflix seems to know exactly what show you'll want to watch next? Or how YouTube's "Up Next" video is often exactly what you were curious about? These algorithms use "collaborative filtering". If you watched a documentary about space, and millions of other people who watched that documentary also watched one about the ocean, Netflix will recommend the ocean documentary to you. The AI has learned patterns from billions of viewing decisions.

But it goes deeper. These algorithms also track what you watch and for how long, when you watch, what you skip or rewind, and similarities to content you've liked. Netflix knows what you'll probably watch next better than you do. YouTube's algorithm is so good that the average user spends over 40 minutes per session. Amazon's recommendation engine drives 35% of their total sales which translates into billions of dollars from AI suggesting "customers who bought this also bought that."

This is pattern recognition from Part 2 working on a massive scale, on major steroids, demonstrating all Four S's: Scale, Scope, Speed, and Subtlety. And just like social media, these engines create their own filter bubbles. They are great for discovering content within your interests but limiting your exposure to different genres, perspectives, and products.

Dynamic Pricing

Now for the part that might make you a bit angry: algorithms that change prices based on your behavior. You've probably experienced this. You search for a flight from New York to Los Angeles, check the price, think about it, and come back an hour later. Now the price has jumped $50. Or you look at a hotel room, browse a few other sites, return to the original site, and the price is suddenly higher. What's happening?

This is called "dynamic pricing," and it's powered by AI algorithms that track your behavior and adjust prices in real-time. Here's how it works: When you visit a website, it drops small files called "cookies" onto your device. These cookies track what you're looking at, how many times you've visited, what other sites you've checked, and even whether you're using a Mac or PC. Mac users often see higher prices because algorithms assume they have more money to spend. Angry yet?

The algorithm interprets repeated visits as strong interest, signaling you're likely to buy. It then raises the price slightly to maximize profit. Airlines and hotels are notorious for this, but it happens with everything from concert tickets to electronics. The algorithm is making split-second decisions: "This person has searched three times, they're probably committed, let's test if they'll pay more." This is pattern recognition analyzing your behavior to predict your willingness to pay. The good news is that you can fight back. Use private browsing mode, clear your cookies regularly, search from different devices, or use a VPN to mask your location. The algorithm can't track patterns it can't see.

Targeted Advertising

Ever look at a product on Amazon, then suddenly see ads for that exact product everywhere you go online? That's not coincidence, that's retargeting, and it's another algorithm tracking your behavior across the internet.

When you visit a website, those cookies we mentioned don't just stay on that site. Advertising networks track you across thousands of websites, building a profile of your interests, shopping habits, and browsing behavior. Look at running shoes on one site, and suddenly you'll see running shoe ads on Facebook, news sites, weather apps, and anywhere else that displays ads.

The algorithm is simple but effective: if you showed interest once, you're more likely to buy if reminded repeatedly. And it works. Retargeted ads are 10 times more likely to get clicked than regular ads. The algorithm is using pattern recognition to predict that persistence pays off. You might not buy those running shoes today, but after seeing them follow you around for a week, you just might cave in. It’s a little weird to think of pair of shoes following you around.

This is the same AI-powered prediction we've seen throughout this part, just applied to advertising. These algorithms know what you've looked at, what you almost bought, and even what time of day you're most likely to make impulse purchases. And just like everything else, you can fight back with private browsing, ad blockers, and regularly clearing your cookies.

Pattern Recognition: The Common Thread

Throughout this part, you've seen the same principles at work across social media feeds, recommendation engines, dynamic pricing, and targeted advertising. Every single one of these systems is doing what we discussed way back in Part 2: pattern recognition on major steroids. Remember the Four S's? Let's see how they apply to everything we've covered:

> **Scale**: These algorithms analyze billions of data points—every click, view, purchase, and scroll from millions of users worldwide. Your behavior is being compared against patterns from hundreds of millions of other people.
> **Scope**: They're not looking at one variable. They're simultaneously analyzing hundreds of factors—time of day, device type, location, browsing history, past purchases, what you clicked, what you skipped, how long you watched, and so much more.
> **Speed**: All of this happens in milliseconds. By the time your social media feed loads, Netflix shows recommendations, or a price appears on screen, algorithms have already analyzed millions of data points and made predictions about what will work best for you.
> **Subtlety**: These systems catch patterns you'd never notice. They know that people who watch true crime documentaries at 10 PM on weekdays are likely to engage with certain types of ads. They understand that someone searching for flights three times is probably more committed than someone searching once.

This is AI in action—not thinking, not understanding, but recognizing patterns and making predictions with incredible accuracy.

Conclusion

We've come a long way in this series. In Parts 1 and 2, we explored the history of AI and how it works, pattern recognition, the learning, the predictions. In Parts 3 and 4, we saw AI working for your benefit, protecting your inbox from spam and helping you find information with search engines. In Part 5, we've seen how AI algorithms shape your online experience in ways both helpful and concerning, whether it is curating your social media feeds, recommending content, adjusting prices, and following you around with ads.

This is the last time we'll look at AI simply as a tool. Everything we've discussed so far has been about algorithms and AI systems built by legitimate companies trying to keep you engaged, sell you products, or provide services. Even when these systems feel manipulative, like dynamic pricing or endless scrolling, they're operating within legal boundaries, and you can protect yourself with the tools we've mentioned: private browsing, clearing cookies, ad blockers, and awareness.

But now we need to shift our focus. Because everything you've learned about how AI recognizes patterns, predicts behavior, and influences decisions, the bad guys know all of this too. And they're using these same AI tools and techniques for something far more sinister than showing you cat videos or raising flight prices.

In Part 6, we'll explore how hackers and cybercriminals are weaponizing AI to steal from you. They're using AI to create phishing emails that are nearly impossible to distinguish from legitimate messages. They're generating deep-fake videos and voice recordings that sound exactly like your CEO, your bank, or even your family members. They're using algorithms to identify the perfect moment to strike when you're most vulnerable to clicking a malicious link or providing sensitive information. The same pattern recognition that recommends your next Netflix show is now being used to predict which scam will work best on you. They aren’t just using AI and algorithms, they are also using your human emotions, something AI cannot predict.

This is why we started KnowPhishing.com. Understanding how AI works isn't just interesting, it's essential for protecting yourself in a world where criminals have access to the same powerful tools as the biggest tech companies. Our free weekly newsletter breaks down the latest threats, explains how scammers are using AI, and gives you practical steps to protect your data and your identity. No technical jargon, no fearmongering, just clear, actionable information to keep you safe. Head over to our website and sign up for our weekly newsletter.

The evolution of AI from simple algorithms to sophisticated learning systems is complete. Now we need to talk about what happens when that power falls into the wrong hands. Thank you for your "attention”, you're going to need it for what comes next.