How AI protects people from online scams

By **Kayla Matthews** - June 26, 2019

4 min read

The internet enables people to connect with friends and colleagues, perform research, enjoy streaming content and more. It has also become a playground for scammers on the lookout for people who will believe their tempting but false offers.

Take the real-life example of a man who fell for the same airline ticket scam twice and lost $1,350 in a week. Frustrated by his American life, the victim decided to take a two-month vacation to Italy and fly business class to get there.

But, not content to pay full price for the tickets, he headed to Craigslist in search of people willing to sell him their frequent flyer miles that he could redeem for his trip. In short, he found two separate scammers who convinced him to pay for their miles — through Western Union and a Green Dot gift card, respectively. One of the scammers even sent the man a contract, presumably to increase his authenticity.

Both parties stopped responding to the buyer once they received his payment, and the victim ended up wasting over $1,000 with no business-class tickets to show for it.

No solution can absolutely prevent future scams like these, although artificial intelligence (AI) has proven its potential so far. AI offers fascinating applications in industries ranging from healthcare to marketing.

Because it spots patterns and trends that humans may miss, and can deal with gigantic amounts of data at once, the technology helps stifle the efforts of online scammers by alerting humans to unusual activity they can investigate further.

AI finds suspicious-looking domains related to tax sites

It's impossible to put all online scams into neatly defined categories, but many of them capitalize on fear or target people who are under pressure. That's why it's no surprise that some cybercriminals create realistic-looking tax sites, such as those with branded elements that claim to offer tech support. In those cases, the websites have a phone number for people to call for assistance.

The people posing as tech support workers then ask for remote access to callers' computers. Instead of fixing anything, though, they steal information or entice a person to install something that will hurt their machine.

Many of the websites that scam people have elements that make them seem official to an unsuspecting individual's eyes.

Sometimes, seeing the brand name in a URL is enough to make a person believe the trick, particularly if they're panicked due to the usual stress of filing taxes. A cybersecurity company called Lookout used an AI tool built in 2017 to look for suspicious domains that could have connections to phishing sites.

When it finds some — related to tax sites or otherwise — Lookout notifies the companies that phishing perpetrators impersonate. Then, those bogus sites get shut down sooner than later, making it less likely that people believe they're legitimate.

AI protects people who are looking for love

The internet gives easily accessible options for people seeking romantic relationships. Although it's certainly not true for all users, some romance-seekers on those sites are desperate, lonely or otherwise feeling emotions that may make them overly eager to jump into partnerships with people they've just met.

Online dating scammers find people to bilk by setting up fake profiles, engaging with users and grooming them for maximum receptiveness. The scammers eventually ask their victims for "loans" of money that they never return.

Researchers in the United Kingdom developed an AI algorithm that spots these fake dating profiles and users and only has a 1% false positive rate. People still need to exercise good judgment when talking to people online, but thanks to AI, such scams could become less worthwhile for scammers to try. This is especially true if their profiles quickly get shut down by dating site operators after alerts come through.

AI stops dangerous emails from reaching their destination

Many internet security companies keep hackers at bay with their in-house AI tools. For example, Trend Micro has a solution that detected more than 66 billion threats in 2017, more than 85% of which were emails with malicious content. Similarly, Google's AI tool for Gmail users is so efficient that it blocks 100 million spam messages each day.

People can generally still see the blocked messages by going into their spam folders. However, since they never get into the email folders that people see most often, there's less of a chance that people fall for tricks. As such, AI could thwart attempts from lottery scammers that urge victims to give details so they can claim "prizes."

These scammers use a false sense of urgency to get people to act. For example, they might say that a person needs to provide their details — which typically include bank account specifics — within 24 hours to avoid having the winnings go to someone else. The scammer might give the impression that they already have the person's details but need the individual to confirm them.

AI tools that filter out scam messages are crucially necessary, especially considering how frequently some people use email to communicate. Additionally, many people — especially the computer illiterate ones — don't know the signs of scam emails, making these filters even more important.

AI safeguards retailers and credit card companies from fraud

Retailers and credit card companies need fraud detection tools in place to make it easier to spot instances of suspected financial fraud — especially those originating from online shoppers. AI helped those entities move beyond manual checks to a more automated system. Most use machine learning, a subset of AI, to learn the differences between normal card transactions and the outliers that could be problematic.

Machine learning systems analyze vast collections of data points that go far beyond what manual methods achieve. They look at historical data and find patterns associated with fraud, then use that knowledge to improve current methods of fighting it.

A 2017 study by LexisNexis found that every dollar of fraud costs U.S. retailers $2.66. Plus, the amount is even higher ($3.46) for retailers that primarily conduct business through digital or remote channels. Curbing fraudulent buying behavior on the internet or elsewhere aids a business's bottom line.

However, some fraud detection methods are overly sensitive. They make legitimate purchasers feel frustrated when they make a large transaction or buy something in an unusual location, and the sales are declined as they try to finalize the purchases.

MIT researchers developed an AI algorithm that could reduce the likelihood of that happening while still keeping retailers safe. It reportedly cuts down on false positives by 54%. Even better, it found some instances of genuine fraud better than existing algorithms.

AI can detect fake restaurant reviews

The internet makes it easy for people to go online and get reviews of restaurants in minutes. They assume that the feedback comes from people who dined at those places. However, some reviewers get paid to publish fake content about places they've never been to. Experts say it won't be long before there's a widespread trend of AI algorithms that can do the same.

A team at Aalto University wanted to deploy AI to help find the fake reviews. Other researchers have attempted the same, but run into some challenges. This attempt involved a technique called neural machine translation that helped give the AI a sense of context.

First, the researchers asked humans to differentiate between real and machine-generated reviews. It found that people interpreted the fake reviews as the actual ones up to 60% of the time. After that, the team developed a classifier tool to detect the fakes. They concluded that it performed exceptionally well in cases where humans could not tell the false from the real.

Being scammed by an unauthentic review arguably is not as severe as some of the other problems mentioned here. However, it could leave people feeling disappointed and misled.

AI keeps online scams at bay

This overview shows that AI has abundant potential for keeping people safe from internet-based scams.

The methods used to combat the problems will inevitably evolve and get more advanced as time goes by.

Kayla Matthews

Kayla Matthews is a journalist and writer focusing on consumer technology, smart homes and the Internet of Things. Check out Kayla's latest projects on her About Me page.