How can our habits of thinking make us vulnerable to deception? What characteristics of information make it more likely to manipulate us? And how can we spot deception before it’s too late? In this episode of *Under the Cortex*, Daniel Simons and Christopher Chabris join APS’s Ludmila Nunes to answer these questions and more, drawing from their brand new book: *Nobody’s Fool: Why We Get Taken In and What We Can Do About It*.

Daniel Simons is a cognitive scientist and professor of psychology at the University of Illinois, where he researches the limits of human awareness and memory. Christopher Chabris is a cognitive scientist who has taught at Union College and Harvard University. In 2010, they co-authored the best-selling book *The
Invisible Gorilla: How Our Intuitions Deceive Us, in which they wrote about cognitive illusions.

Unedited transcript:

[00:00:10.490] – Ludmila Nunes

Daniel Simons is a cognitive scientist and professor of psychology at the University of Illinois, where he researches the limits of human awareness and memory. Christopher Chabris is a cognitive scientist who has talked at Union College and Harvard University. He teaches about behavioral and decision sciences. In 2010, they coauthored the best selling book The Invisible Gorilla: How Our Intuitions Deceive Us, in which they wrote about cognitive illusions. Two days ago, on July 11, they released their new book Nobody’s Fool: Why we Get Taken In and What We Can Io About it? In this book, they describe how our habits of thinking can make us vulnerable to deception, the characteristics of information that make it more likely to manipulate us, and they also provide some practical tools we can use to spot deception before it’s too late. We invited Daniel Simons and Christopher Chabris to speak about their new book. This is Under the Cortex, and I’m Ludmila Nunes. Dan and Chris, thank you so much for joining me today.

[00:01:17.610] – Daniel Simons

Thanks for having us on.

[00:01:19.120] – Christopher Chabris

Yeah, great to be here.

[00:01:21.210] – Ludmila Nunes

So in your new book, Nobody’s Fool You, show us how to spot and avoid scams and other deceptions. What inspired you to write this book?

[00:01:31.150] – Daniel Simons

Well, I’ll start. After we wrote The Invisible Gorilla, we really enjoyed the writing process, we really enjoyed the research process, and we always wanted to write another book. And over the ensuing decade or so, we gathered a lot of material that we found really interesting. And the key question for us was how we could put it together into a unifying theme. So The Invisible Gorilla was all about how our own intuitions about our minds are often misleading and incorrect because they’re based on partial or incorrect information. We don’t always understand how our minds work, and for good reasons. This book is more about how our cognitive tendencies and habits and the information we find really appealing can be used against us, even though most of the time they’re really effective. So whereas The Invisible Gorilla was more about how we sort of don’t understand the workings of our own minds, the ways in which that can lead us astray, this book is much more about how our tendencies that work well, the vast majority of the time can be hijacked under the wrong circumstances.

[00:02:35.010] – Christopher Chabris
The other thing that this book does, which I think is unique, is that in all the movies and podcasts and articles and so on about scams, they all talk about what the scammers did and how they were caught and how the victims felt about it and what the victims wound up doing. But none of them really explain why people keep falling for this stuff. There’s some good work on that that’s come out, but it’s pretty rare. And we wanted to sort of take a cognitive psychology approach and sort of hold up what we know about how the mind works, up against sort of all these patterns of the kinds of scams and cons and frauds and misinformation that work year after year, decade after decade, and see what patterns we could see, and come up with a framework for understanding why deception works, why fraud keeps on working for centuries. Millennia. Back to the Trojan Horse. And then maybe, as Dan said, sort of distill from that some ways that people can think smarter about this kind of stuff before they get sucked in.

[00:03:32.160] – Daniel Simons

The same things has continued to work over the decades. We don’t seem to learn from these, even though we’ve watched them over and over and over again.

[00:03:39.670] – Ludmila Nunes

And so your book has two parts. One is called habits. The other one hooks in habits. You write about the cognitive habits that we all have, and we have them because they serve a function. They usually work in our favor and help us navigate the world and make sense of it. But the issue is that these habits can be exploited by those who are looking to fool us. What are these habits? Do you want to talk about a few of them, what they have in common?

[00:04:11.570] – Daniel Simons

Sure.

[00:04:12.290] – Christopher Chabris

We have four of them. I think one of the ones that’s most interesting to mention is efficiency. So efficiency is the habit of making decisions based on as little information as we can, as quickly as we can. You could think infinitely about any decision you wanted to make. You could keep on gathering information, you could keep on turning it over in your head. I personally tend to do that a little bit too much when playing chess, for example, and then I run out of time and I play poorly. But in daily life, we’ve got to make lots and lots of decisions based on very little information. So we strive for efficiency. But the problem there, of course, is that in a situation involving deception or someone trying to fool us, we may not have all the information we need to figure out that that’s what they’re doing. And the drive for efficiency can lead us to make a decision based on an inadequate amount of information. And the solution to that is not completely trivial to adopt, but it’s easier, I think, than it might appear. It’s often just to ask one or two more questions before making a final decision.

[00:05:10.540] – Christopher Chabris

So when you feel yourself ready to make a final decision about something important, like not about which can of peas to buy in the supermarket or something like that, but for example, which money
manager you’re going to put in charge of your life savings? Ask a couple more questions before you take the final step, just for one of the most humorous examples along these lines is the crypto currency company FTX was trying to get a lot of celebrities to endorse them and Tom Brady, I think, made a Super Bowl ad for them. But Taylor Swift was one of the ones that they approached and turned them down. And apparently that was because she asked them, aren’t you guys basically selling unregistered securities here? That’s one of the things that they are accused essentially of having done, or at least suspect of having done. And by asking that question, she avoided becoming one of their endorsers and potentially being legally liable for anything that went wrong with customers after putting her name to it. So sometimes just one more question, if it’s the right one, can overcome the efficiency habit.

[00:06:03.290] – Daniel Simons

Yeah. And those who are looking to capitalize on this habit just to kind of hijack it in their favor, often will put huge time pressure on you. They’ll make it an urgent situation when in reality, there are very few things that are truly that urgent. But when you’re under a lot of time pressure, you want to act as efficiently and get out of that pressure as quickly as you can. And of course, people looking to con you know that. So those sorts of people who are doing high pressure sales tactics, they’re going to keep you trying to respond quickly, that you’re going to lose out on an opportunity or you’re going to face a giant risk if you don’t respond immediately. And in that context, taking a step back and asking a question is just a way of slowing things down a little bit, realizing, do I really need this kind of time pressure? More often than not, that’s a sign that somebody’s trying to take something out of you.

[00:06:48.850] – Ludmila Nunes

So maybe one of the first strategies is if someone is asking you to make decision very quickly, just stop and ask questions because that might already mean that there’s something fishy going on.

[00:07:02.760] – Daniel Simons

Yeah. I mean, how often is there a true high pressure deadline without much warning? Right. How often do you get a call and say, you have to do this right now and there’s no choice? That almost never happens. Yeah.

[00:07:15.690] – Ludmila Nunes

Then do you have a favorite habit too?

[00:07:18.430] – Daniel Simons

I’m not sure I’d have a favorite. I kind of like the idea of prediction, and this is related to the idea of confirmation bias, that we tend to look for information that matches what we hope to see, what we expect to see. But it has a more broader principle, right. Most of the time that’s a really useful thing to be doing because we have to anticipate what’s going to happen around us in our world all the time. And most of the time that’s a good thing to do because it makes us more efficient and able to process the information that’s coming in. But it plays into a lot of aspects of deception, including unintentional deception that we might inflict on other people. So take for example, you see a story posted to social
media and it fits what you expect. It’s kind of along the lines of the sort of things that you believe. So when that happens, we don’t tend to check it. Instead, we tend to forward it. It’s because it’s what we predicted. And of course, if you feed people what they expect to see and they amplify it by forwarding it without thinking about it, that leads to the spread of misinformation.

[00:08:18.850] – Daniel Simons

This plays a huge role in unintentional scientific deception. So think about what would happen if you run a study. You conduct a study and the data look perfect. Everything lines up exactly as you expected it to. You’re probably not going to dig into the data to make sure you didn’t miscode something to the extent you would if it came out exactly the opposite of what you expected. If that happened, you’d dig in, you’d see, did I miscode the conditions? Did I get things backwards? And you’d be more likely to spot errors in things that didn’t match what you were looking for than things that you did. If you don’t have a systematic process that forces you to say, okay, I’m always going to check my data and make sure that everything’s coded correctly, then what’s going to end up happening is things that are consistent with your predictions go right along without error checking, and things that are inconsistent get checked much more thoroughly. And that can lead to mistaken information, mistaken inferences about the science. It’s one of the reasons why larger collaborations are really effective, especially if they come with different viewpoints, that you can have people who disagree with you double checking you and making sure that they find the results compelling as well.

[00:09:24.710] – Ludmila Nunes

So in the second part of the book, you talk about hooks and describe features of the information we are exposed to that can spike our interest and therefore make us accept it without actually checking the information. What are these hooks?

[00:09:42.650] – Christopher Chabris

Well, I would start with consistency, which is, I think, one of the first ones we talk about in that section. Consistency refers to the idea that when there’s not very much noise in a set of data and I’m speaking very generally, not necessarily a series of numbers you’re looking at but whenever things seem sort of consistent, smooth lines going straight up, things being completely equal or identical or symmetrical, we tend to take those things as signs of trustworthiness, credibility, accuracy, truthfulness. And sometimes that’s true, right? So a really good scientific experiment will get the same results every time. If it’s based on a good theory and sound methodology and so on, you will get consistent results. But in data involving human activities, from clinical trials to behavioral experiments to larger scale systems like the stock market, there’s a lot of noise in the outcomes. The day to day fluctuations in stock prices, the month to month fluctuations in stock prices. One of the red flags that people could have noticed or picked up on in what Bernie Madoff was doing with his fake hedge fund, his Ponzi scheme, was that the returns were too consistent.

[00:10:55.790] – Christopher Chabris

Every month every year, people made about exactly the same amount on their money, eight to 12% very small fluctuations. And it might be what you would expect from bonds or treasury bills or something
like that. But if someone claims to be investing in the stock market, they can’t achieve that. It’s too consistent. And other people did notice that. And that’s one of the things that the whistleblowers about the Madoff case did notice. They said, these returns are impossible. Many everyday investors, and even some more sophisticated ones didn’t notice that. So the consistency could have been a red flag to, is this real? Like, is this being generated by really what they say it is? And you could apply that in other contexts as well as beyond finance.

[00:11:35.430] – Daniel Simons

We tend to think of noise as a bad thing, but often it’s exactly what we should expect. So in science, one of the more commonly discovered kinds of fraud comes from randomized clinical trials, where you take a group of people and you randomly assign some of them to the experimental treatment group, the drug or the intervention, and others to a placebo group. And when you do that, you want to make sure that the groups are otherwise equal. So for in a medical trial, you’d want to make sure that there wasn’t a huge disparity in prior health problems between the placebo group and the experimental group. And in an ideal world, they’d be equated. But randomization doesn’t lead to them being equated. So if you do this and you try and equate people on a whole bunch of different sorts of things just through randomization, you won’t expect them to all be equal between the placebo group and the treatment group. And in fact, if they’re all too close together, if the differences between the groups and all of these other metrics are too small, that’s a sign of fraud. It doesn’t happen by chance. So looking for that sort of variability and noise is actually a sign that it was genuinely done the way people said it was done.

[00:12:42.930] – Daniel Simons

And we don’t often realize that. We tend to think, oh, this is so perfect. I don’t want any differences between my groups. And a fraudster says, I don’t want any differences between my groups. So they make everything perfectly consistent across all of the metrics. And in doing that, they reveal themselves as frauds.

[00:12:56.510] – Christopher Chabris

Yeah, I just want to mention familiarity also, which is one of the other hooks, because I think it’s kind of underappreciated. Sometimes we tend to be attracted to what’s familiar and what’s similar to what we’ve experienced before. And this can be used in sort of interesting political manipulations, even, for example, running. They’re called ghost candidates. So there’s a story of two Rodriguez’s who both ran for the same office in Florida. One was a legitimate candidate, one was this kind of ghost candidate. In fact, I think they were both named Alex Rodriguez, if I recall correctly. Also the same name as a famous baseball player. So this kind of thing, due to the familiarity of the names, similarity to familiar names, can actually have consequences and mislead just enough voters to make a difference in the final outcome of the election.

[00:13:44.550] – Ludmila Nunes

And this is not because people are not able to reason or people are not good at thinking. Actually, in your book you write that people who are better able to reason can actually be more easily fooled when they’re motivated to justify their beliefs.
I think there’s a real danger when watching all of these sort of documentaries about cons that in hindsight they’re obvious and we can see the victims of them as more clueless, more naive, more gullible than the rest of us. It’s easy to do when you’re not immersed in a deception that’s targeting you. But a lot of the sort of examples that we talk about throughout the book are of people who are at the tops of their professions being fooled. And if you look at the board members of theranos the biotech company that is now disgraced, they were former cabinet secretaries, retired generals. I mean, these are accomplished, educated, smart people who are falling for a con.

Yeah, we all have these I’m going to call them fallacies.

I like tendencies better because fallacies implies that they’re inherently bad. The vast majority of the time they work great and it’s only when people hijack them that they cause problems. And that’s relatively rare.

Most cons and scams and frauds, especially ones that take a lot of money, last for a long time and get made into documentaries, rely on a lot of these habits and hooks. So Madoff was sort of using them all. So in the way we think of it, we have them as separate categories, but often they combine and they interact. And the point is not that sort of every single con or scam is doing one of these things, but that they’re using various combinations of these things and in fact, maybe recombining them in new ways. So we think that they’re going to use a lot of the same habits and hooks that we identify.

And we talked about how to be more aware and potentially avoid being taken advantage of. And one way is being more aware, trying to stop and think before making a decision and be also aware of our own expectations of familiarity and how this can be used to trick us. Do you have any other advice?

Sure. I mean, there are some things that you can do in advance rather than trying to react in the moment when you’re under time pressure or in a potentially difficult situation. Anticipating cases where you might be fooled or where you want to check more can be a good way of doing it. There’s a famous story from the rock band Van Halen that in their concert rider for their concerts, they would demand that their room have a bowl of M and Ms, but with no brown M and Ms. And it wasn’t that they didn’t like brown. It was that that was just a simple check on whether people were being careful and consistent in checking what they required. So the first thing they do is go into the room, see if there are any brown M and Ms. If there are, they know that people aren’t paying close attention to their instructions, and then they should be much more attentive to things like their rigging and pyrotechnics that could actually hurt
people. Whereas if they did follow it, that’s no guarantee, but it at least shows that people are paying attention to the details. There are other contexts in which you can do this sort of thing, too.

[00:17:06.630] – Daniel Simons

So a common scam right now involves calling people up and pretending to be a kid, or somebody calling on behalf of a kid, calling a grandparent or a parent and saying, your kid’s been in an accident, or We’ve kidnapped your kid. These are really horrible scams, and they put you under huge pressure to send money right away. So one thing you can do to kind of preemptively prevent that is have a family passcode so that if there’s that sort of situation, all you do is say, okay, what’s the code? And if they don’t give it to you immediately, you know that it’s a scam, and you can just hang up. So that’s something you can do preventatively rather than having to evaluate in that moment and get somebody when under pressure to answer questions. So that’s, I think, a good tactic, but really just checking a little bit more when there might be a risk, and knowing that time pressure is rarely that genuine can help a lot.

[00:17:56.940] – Christopher Chabris

A good way of checking also is to use someone else. So one of my favorite stories that we learned in this process was about a scam, really, that ran in Europe for a while, where some guys pretended to be the French defense minister, believe it or not, and would contact various wealthy people and ask them for money to help them pay ransom to ISIS in Syria and Iraq to get back French hostages. And when the victims of this con would say, oh, I didn’t hear about any hostages, the fake defense minister would say, oh, well, it hasn’t become public yet. We’re trying to work behind the scenes. And if they said, well, why doesn’t the government just pay for this? You’re the government of France. They would say, well, it’s not in our budget. We want to keep it secret. We don’t want to make this public that we’re paying the ransom, and so on. So we need your help, and you’d be doing a great service to the Republic. And they even went so far as to have text mask created that would make them look like the French defense minister. They should do skype calls.

[00:18:50.870] – Christopher Chabris

So there was one wealthy businessman who was basically about to agree to wire money to these fraudsters to get some fake hostages out of Syria or something, when his friend walked into the room where he’s having this Skype conversation and immediately says, like, this is a scam. So you don’t have to wait for your friend to wander in. Right. If it’s a big decision, you could say, could you take a look at this for me? It practiced, known sometimes as red teaming. You actually ask someone to take a critical eye, like, look at this and try to explain to me why I’m making a bad decision, or what would be the argument against doing what I’m doing, and then try to evaluate that as objectively as you can before you make that big commitment.


Yeah. In science, for example, you can take preventative steps to make sure that fraud doesn’t happen from people you have to trust. Right. So any of us who are scientists and have students who work with us, there has to be some degree of trust between students and colleagues. But if you just rely on that
trust, that does lead to the potential for somebody to take advantage of it. So there are lots of things you can do. One is to have two people in your lab analyze every data set independently, see if you get the same results. And it might just be that you detect errors that way. We often do. So I’ll often reanalyze data that a student generated. They’re learning to calculate stuff. Everybody makes mistakes, and we can often catch each other’s mistakes and get them fixed. But it’s a way, without actually imposing on somebody or threatening them or challenging their trust to make sure that everything’s good. So if you make it part of your standard process, it becomes like the bowl of brown M and Ms. It makes sure that everything is what you hope it is, and you end up with the same results each time, then that’s good.

[00:20:29.040] – Ludmila Nunes

So it was great speaking with you.

[00:20:31.360] – Daniel Simons

Yeah, it was great chatting with you.

[00:20:32.640] – Christopher Chabris

Same here.

[00:20:36.810] – Ludmila Nunes

This is Ludmila Nunes with APS, and I’ve been speaking to Daniel Simons and Christopher Chabri, authors of the book Nobody’s Fool: Why we get taken in and what we can do about It. Find out more about APS at psychologicalscience.org.