Booking.com sounds alarm on AI-enabled travel scams

June 20 2024, by Alex PIGMAN

Marnie Wilking, the chief information security officer of Booking.com is photographed during an interview at Collision 2024 in Torontoon June 18, 2024.

As travelers rush to book their summer getaways, Booking.com's internet safety boss says watch out for supercharged AI scams.

Marnie Wilking, Chief Information Security Officer at the Netherlands-based travel giant, said generative AI had sparked an explosion in online phishing scams, and that the hospitality industry, long spared, had also become a target.

"Over the course of the last year and a half, throughout all industries, there's been anywhere from a 500 to a 900% increase in attacks, in phishing in particular, across the globe," Wilking told AFP on the sidelines of the Collision technology conference in Toronto.

Phishing scams are a type of cyber attack where criminals attempt to trick victims into revealing sensitive information such as login credentials or financial account details.

Travel websites can offer a rich bounty to phishing scammers since travelers are often asked to share credit card and family details or upload ID.

"Of course, we've had phishing since the dawn of email. But the uptick started shortly after ChatGPT got launched. The attackers are definitely using AI to launch attacks that mimic emails far better than anything that they've done to date," she said.

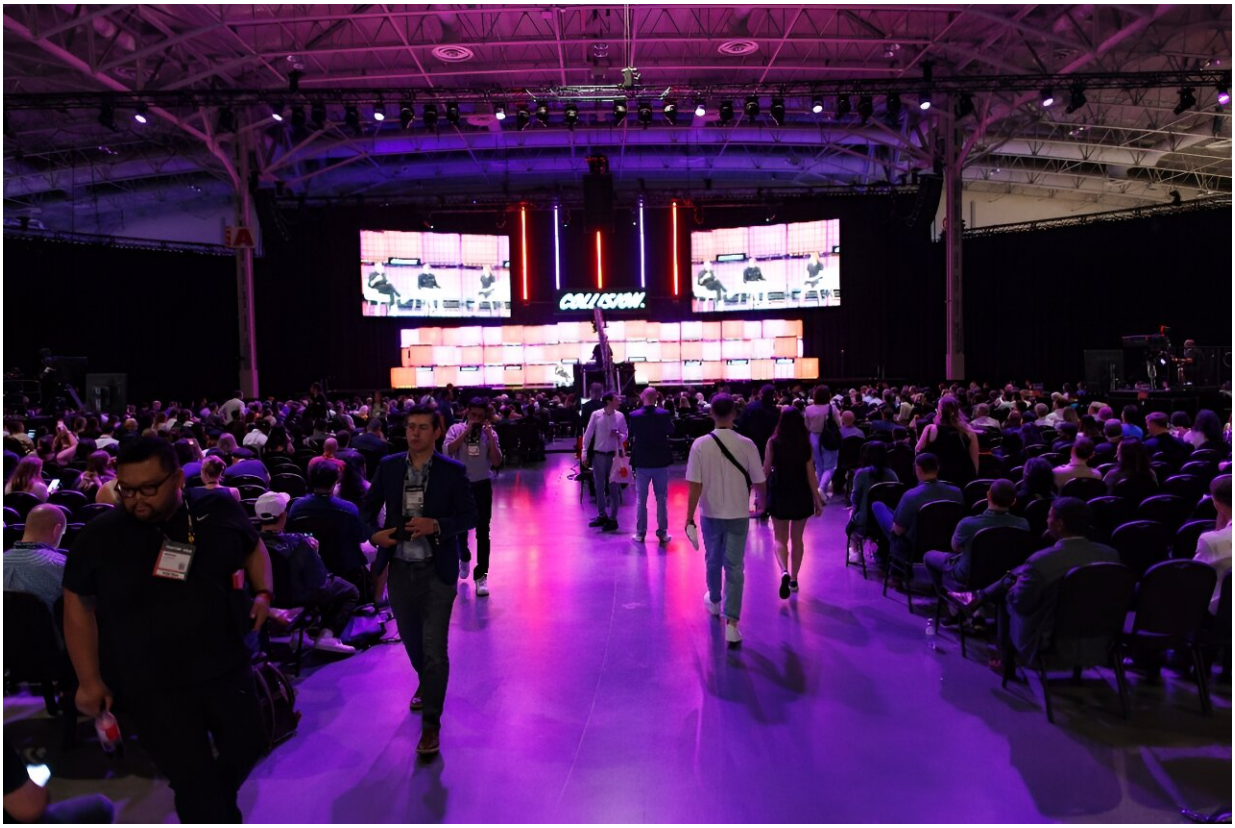
With generative AI tools, the scammers can now work in multiple languages and with good grammar, Wilking said.

They are also "really taking advantage of the helpful nature of hospitality."

To be helpful to a supposed guest, a hotel owner is "probably going to open up the attachment" that is actually malware, she said.

Wilking said that in order to stay safe travelers and hosts should sign up

for two-factor authentication when surfing online.



Attendees watch a panel on the main stage during the 2024 Collision tech conference at Enercare Centre in Toronto, Canada, June 18, 2024.

In addition to providing a username and password, two-factor authentication requires users to verify their identity through an added factor, such as a one-time code sent to their mobile device or generated by an authenticator app.

"I know it can be a little bit painful just to set up and then you have to remember which phone it's on and everything," she said.

However, the extra step "is still hands down the best way to combat phishing and credential stealing," she said.

And "don't click on anything that looks suspicious, even if you think it might be real. If there's even a little bit of doubt, call the property, hosts, and customer support," she said.

Fake property?

Wilking said Booking.com and other major companies are cooperating closely and increasingly relying on AI to help in the fight.

AI, for example, is helping thwart the proliferation of fake properties on platforms that are actually a bid to scam the user.

Scammers "set up a fake property that looks like it's in the Swiss Alps. Every other property around it is $1,000 a night and this one's on sale for $200."

"We've set up AI models to detect those and either block them from getting on there to begin or take it down before there's any booking," she said.

Though it remains modest for now, travel sites have seen the rise of suspected state actors, reported to be Russia and China, that are trying to cause online mischief or snoop on customers.

"Why would a nation state go after a hotel chain? Well, if it's a hotel chain that they know is frequented by a US senator, why wouldn't they go after that?" she said.