+44 345 094 0945
www.waterstons.com

Article

Dec 2025

When travel booking goes south

Thousands of fake travel-booking websites have been created to trick users into revealing payment details.

What happened?

A Russian-speaking cybercrime group has spun up over 4,300 bogus travel-booking sites, impersonating trusted brands like Booking.com and Airbnb. Victims received emails asking them to confirm or update their reservation, a classic psychological trick to create urgency and stop people from thinking twice.

But clicking the link took users to high-quality cloned websites available in 43 languages. These fakes were impressively convincing: familiar logos, polished layouts, and even customer-support chat windows. They went as far as showing fake '3D Secure' verification screens, making everything feel safe and routine while quietly stealing credit card details in the background.

To make things worse, many of these fake sites used valid SSL/TLS certificates (that little padlock icon in the browser), but the padlock only means the connection is encrypted, not that the site itself is trustworthy. Criminals know we have been trained to trust that icon, and they are more than happy to use that to their advantage.

The scale and automation behind this campaign show that even simple, everyday tasks like booking a holiday can open the door to fraud, payment card theft, and reputational damage for both individuals and organisations.

The rise of phishing attacks

Phishing is no longer about clumsy typos and obvious scams, it's becoming industrialised, polished, and heavily automated. Criminals can now:

Clone well-known brands in multiple languages

Register thousands of lookalike domains in bulk

Target sectors where people expect to pay quickly, like travel and hospitality.

When you are trying to grab that last available room or cheap flight before it 'expires', you are more likely to click fast and think later. Attackers know this and build their scams around that sense of urgency and trust.

What we recommend Don't worry, we're not telling you to stop booking holidays! But you do need to book travel a bit more carefully.

Train staff to spot suspicious travel-themed emails and avoid clicking booking links directly from messages.

Bust the padlock myth: remind everyone that SSL/TLS (the padlock) only encrypts traffic - it does not guarantee the site is legitimate.

Use technical controls such as blocking typo/impersonation domains, enabling web-filtering, and monitoring newly registered lookalike sites.

When it comes to cyber awareness, little and often wins:

Short nudges and quick refreshers during busy travel seasons

Regular phishing simulations that feel realistic, not punitive

Fun, interactive learning – research shows it can improve retention by up to six times

Gamified exercises, quizzes, or scenario-based workshops can turn 'yet another cyber training session' into something people actually remember.

Finally, make sure your incident-response plan is ready for this kind of scam. It should clearly set out:

What to do if payment-card details are compromised

How to communicate with affected staff, customers, or partners

How to limit further damage and recover quickly

Enhance your cybersecurity today

If you would like to make sure your next holiday booking does not come with a side order of card fraud, our cyber team can help.

For more information about improving your cyber security and protecting your organisation against these types of cyberattacks, contact our cyber experts at cyberaus@waterstons.com.