



# Online safety checklist for Hosts



We want to help you be able to advertise, take bookings and get paid for stays with confidence.

To help protect you and your earnings, online safety experts and member of Airbnb's UK Trust and Safety Alliance, [Get Safe Online](#), have shared some top tips.

## 1. Only receive payments and communicate via Airbnb

Always stay on the Airbnb platform to receive payments and communicate with guests. This will help ensure you're protected by Airbnb's policies and secure processes like [AirCover](#), and avoid issues like overpayment scams and other frauds.

Use Airbnb's secure messaging system to get to know your guests and communicate ahead of check-in or during their stay.

## 2. Beware of fake emails, websites, texts and social media posts

'Phishing' emails and websites can be designed to appear as if they are from or connected to Airbnb but are, in fact, operated by fraudsters.

Never click on links in emails, texts, social media posts or messages that you're not expecting. These may take you to fake websites designed to capture your personal information or infect your device with malware. If you're approached for a stay from anywhere but the official Airbnb website, it could be a red flag for fraud.

If you're unsure about the authenticity of an email or website containing a link to Airbnb, type the Airbnb website address ([www.airbnb.co.uk](http://www.airbnb.co.uk)) directly into your browser and log into your account from there. If it's genuine and important, you'll usually find more information in your Airbnb account dashboard.

Learn how to identify a genuine Airbnb email address or webpage [here](#). If you think you've encountered a fake Airbnb website, [report it to Airbnb](#) and help protect the Airbnb community from phishing and scams.

## 3. Protect your account

Fraudsters may try to access your account using your login information obtained through, for example, a hack or phishing scam. These are often known as 'account takeovers'. To help protect against this, Airbnb uses 2-step authentication, which asks you for a randomly generated code to confirm your identity.

To help you stay secure online, use a strong, separate password for every account. Find out more about keeping your Airbnb account secure [here](#).

## 4. Get in touch

If you need support before or during a reservation, Airbnb's global Community Support team is on hand 24/7 to assist, and can be reached by phone, in-app, or through the [Help Centre](#).

For more online safety tips, visit [www.getsafeonline.org](http://www.getsafeonline.org)

### Providing wi-fi access to guests? Protect yourself against malicious activity

1. Create an encrypted (ex: WPA2) guest network, and only share that password with guests after they've confirmed their reservation
2. Store your router and modem in a secure, locked location in the accommodation that guests can't access
3. Create strong, unique passwords for your router and modem, and change them often
4. Routinely check your router and modem for software updates
5. Consider including in the guest handbook that if they use your wi-fi network should, they are to use it only be used for legal purposes and are not to use it for uploading or downloading of illegal content or other illicit activities is not allowed

