Holiday Season Online Scams

What are they and how do I avoid falling victim?

Online Scams

Threat actors love to take advantage of people during the holiday season.

Here are the 6 most common online holiday scams and 10 ways to avoid falling victim.

Fake Charity Scams

Scammers create a fake charity or ask for donations to a real charity to trick you into donating money or providing personal information.

They often use emotional language or fake stories to elicit sympathy.

Gift Card Scams

Scammers offer gift cards at discounted rates or as prizes in exchange for personal information or payment, but the gift cards turn out to be fake or they have already been used.

Fake Surveys

Fake surveys offer prizes or rewards for participating but trick people into providing personal information or clicking on malicious links.

These scams can be emails, pop-ups, or social media posts, and may use real branding or logos to make them appear legitimate.

Social Media Scams

These scams use social media like Facebook, Twitter, or Instagram to trick people into providing personal information, sending money, or clicking on malicious links.

Travel Scams

The threat actor offers fake travel deals or packages, often at discounted rates, to trick people into providing personal information or making payments.

Examples are fake airline tickets or hotel booking websites, fake travel agents or tour operators, or fake vacation rental listings.

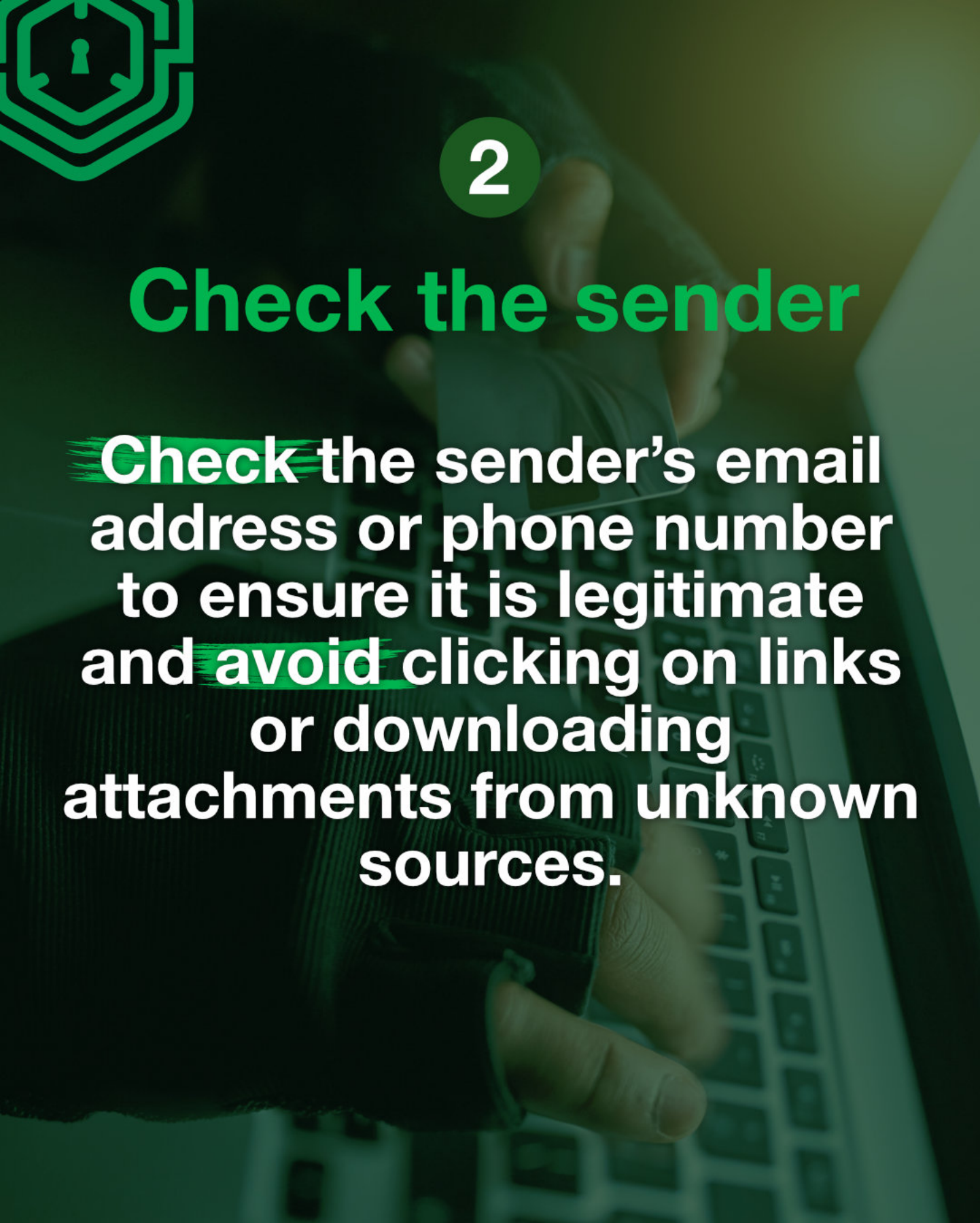
Phishing & Smishing

Phishing is where a threat actor sends a fraudulent message via email to trick the recipient into revealing sensitive information or clicking on a malicious link.

Smishing uses the same technique, but is sent via SMS rather than email.


So how do I
defend against
these scams?


1
Be sceptical
If you receive an email or message from someone you don't know or a company you didn't sign up to receive messages from, be sceptical of any offers or requests they make.



2

Check the sender

Check the sender's email address or phone number to ensure it is legitimate and avoid clicking on links or downloading attachments from unknown sources.

3

Passwords & MFA

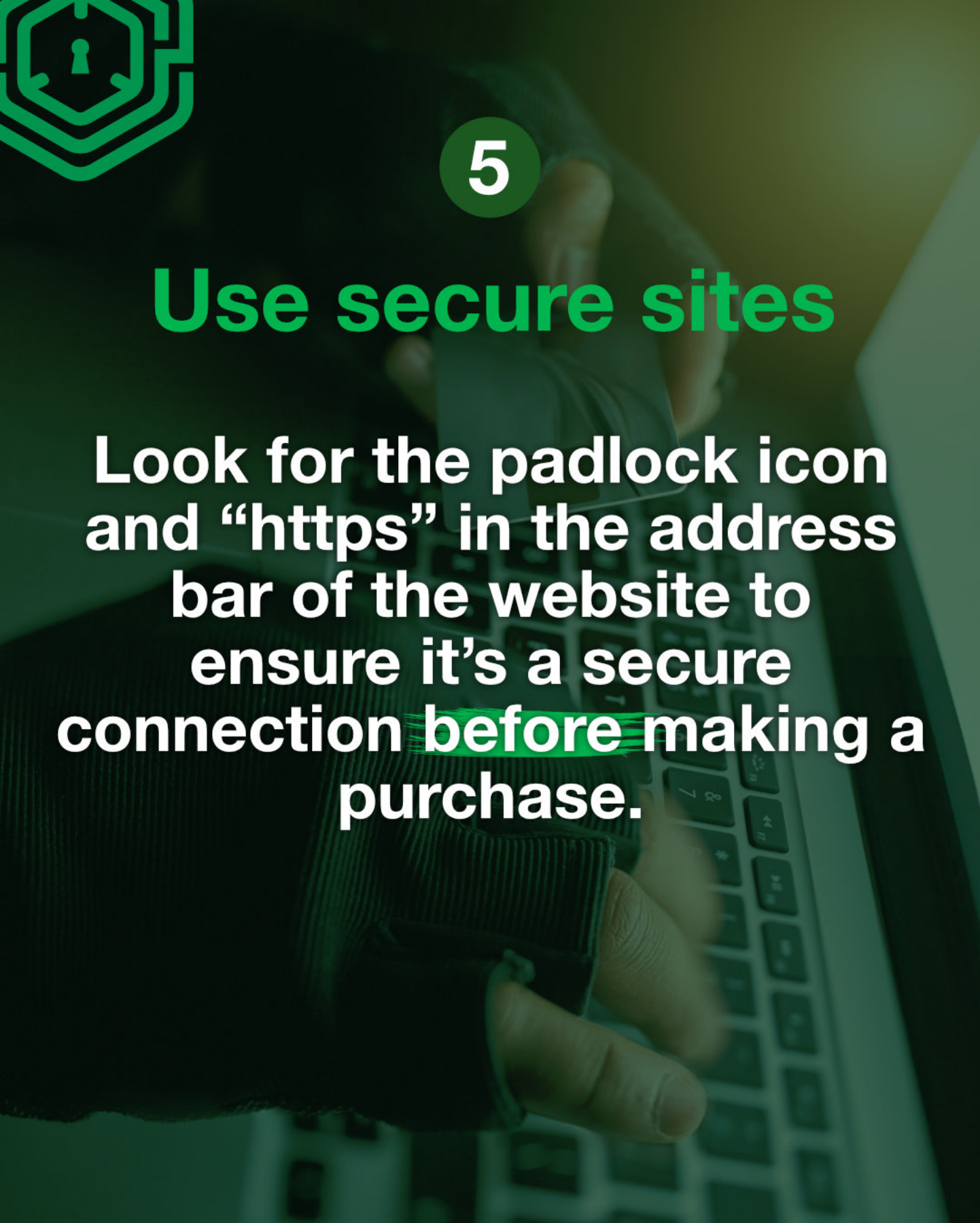
Protect your accounts with strong and unique passwords, and use multi-factor (MFA) authentication when possible.

Don’t reuse the same password across accounts.

4

Anti-Malware

Install anti-malware / endpoint protection software on your devices and keep it up to date to protect your computer or device from malware.



5

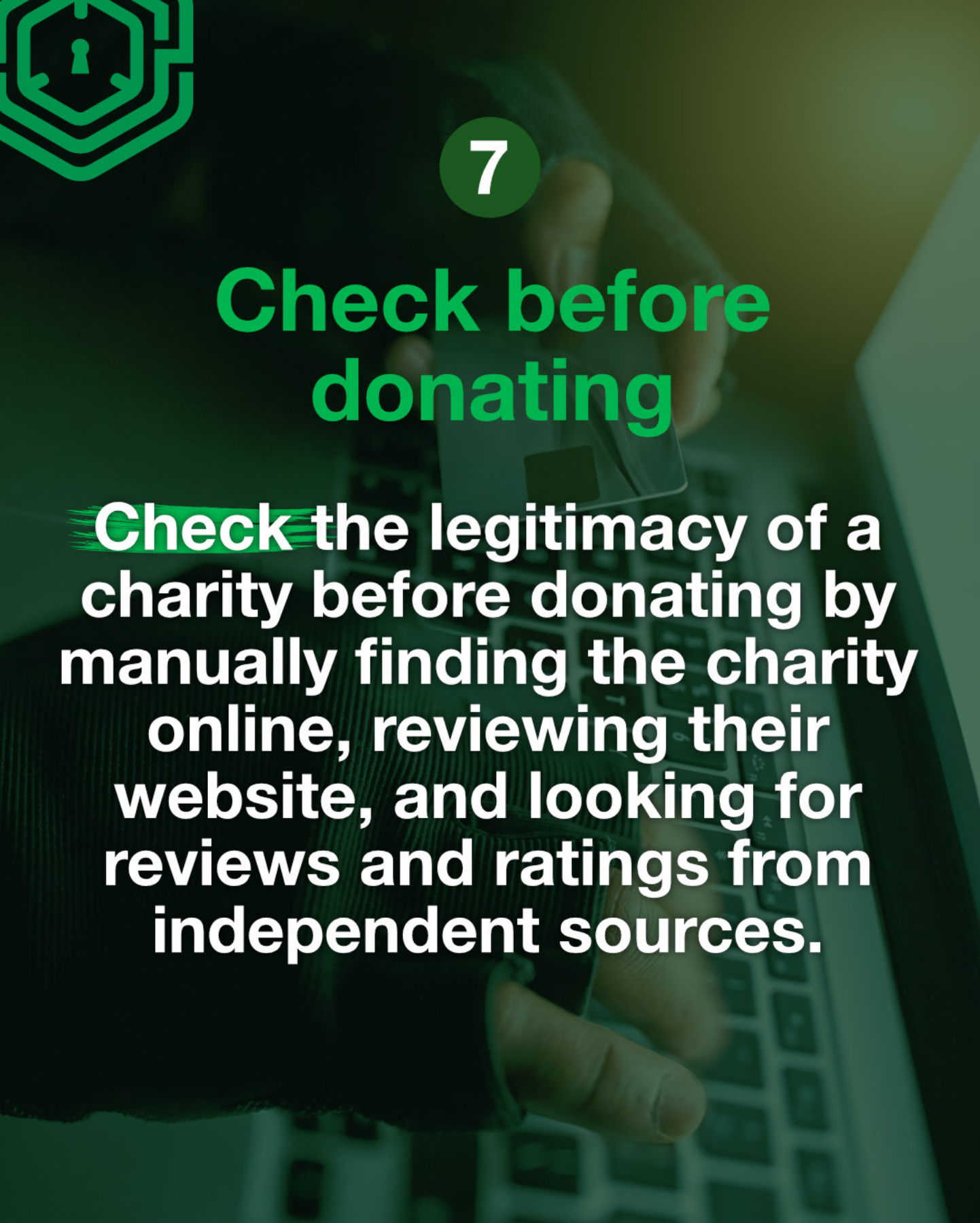
Use secure sites

Look for the padlock icon and “https” in the address bar of the website to ensure it’s a secure connection before making a purchase.

6

Protect your PII

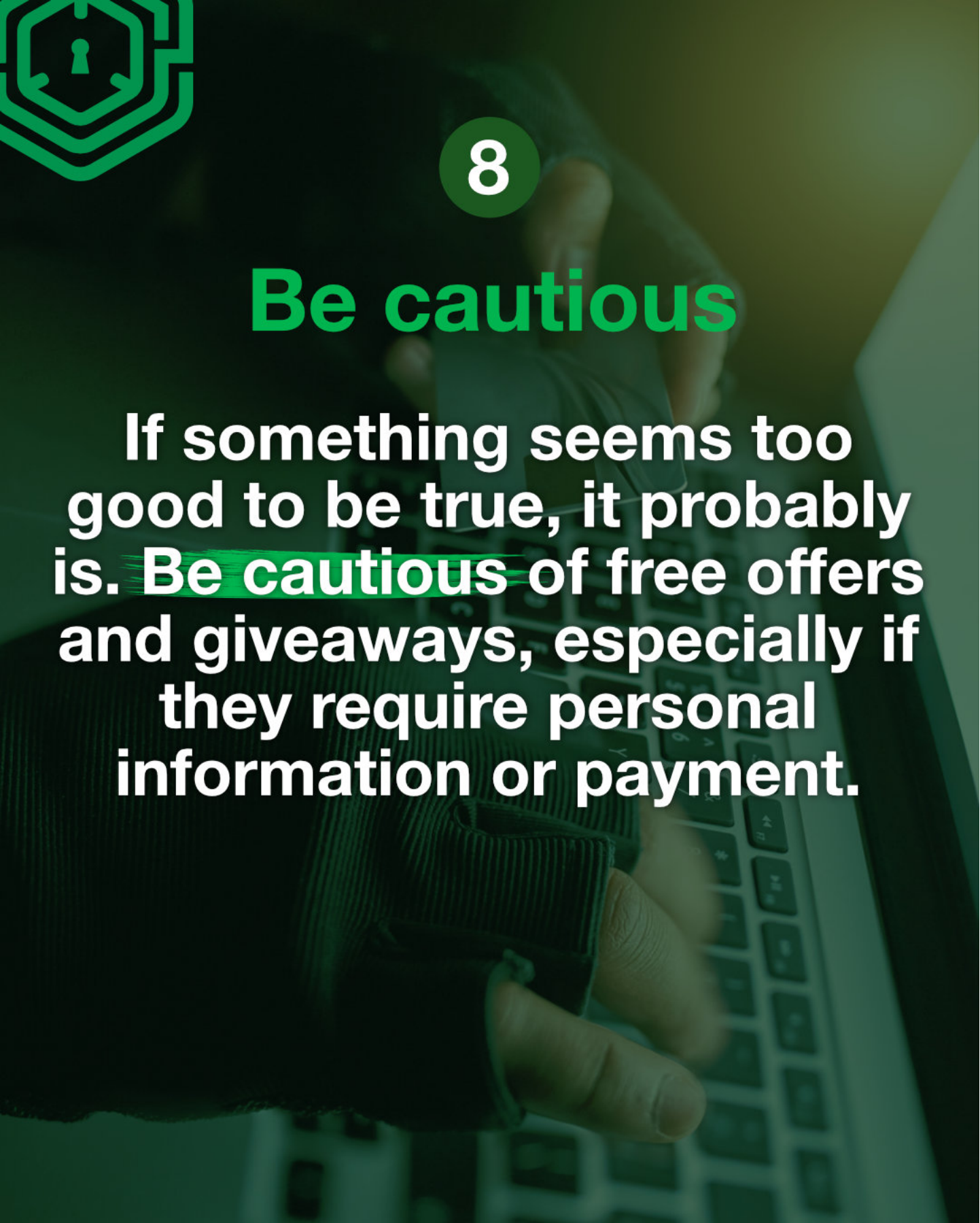
Avoid giving out personally identifiable information (PII) like your birthdate, driver's license, passport, TFN or bank account information unless it's absolutely necessary.



7

Check before donating

Check the legitimacy of a charity before donating by manually finding the charity online, reviewing their website, and looking for reviews and ratings from independent sources.



8

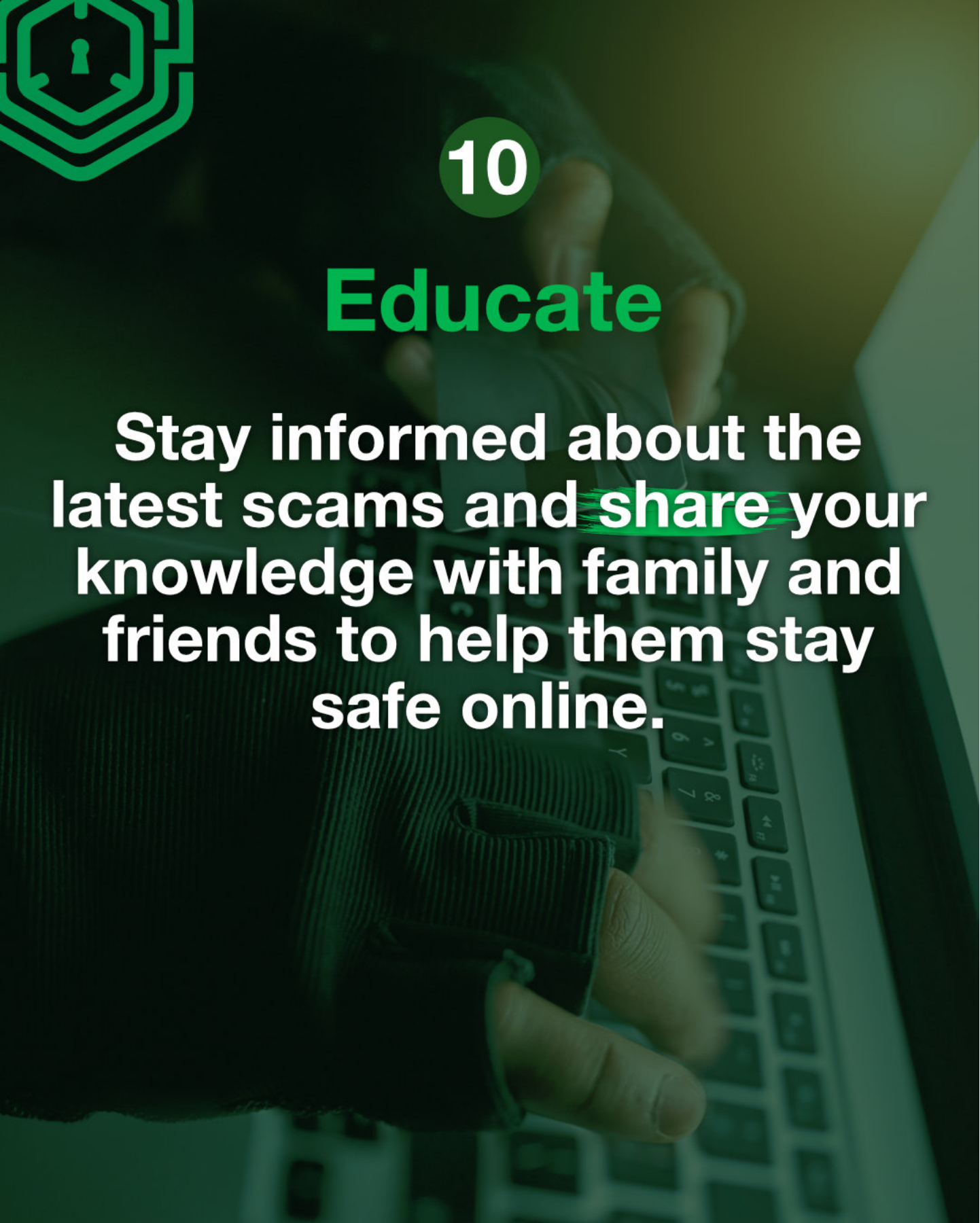
Be cautious

If something seems too good to be true, it probably is. Be cautious of free offers and giveaways, especially if they require personal information or payment.

9

Update software

Keep your operating system and software up to date with the latest security patches to prevent vulnerabilities that can be exploited by scammers and other threat actors.



10

Educate

Stay informed about the latest scams and share your knowledge with family and friends to help them stay safe online.

Want More Information?

For more details on how to protect yourself from online scams, visit our insights page!

https://morrisec.com.au/insights

MORRISEC