HOW TO ENJOY A RISK-FREE HOLIDAY

KEEP FRAUDSTERS AT BAY

Invest in a good anti-virus/ anti malware package to detect unsafe links and applications

Track your payments with Transaction Alerts and contact your issuing company in case of unauthorized activity

Use VPN-services when using public Wi-Fi. VPN will create an encrypted channel for your data

Use your Visa Payments Device Token to protect your payment data from compromise

IF THE OFFER LOOKS TOO GOOD TO BE TRUE… IT PROBABLY IS.

Double check the company's website to see if the offer is legitimate

Make sure that the URL starts with https:// otherwise, it's not secure

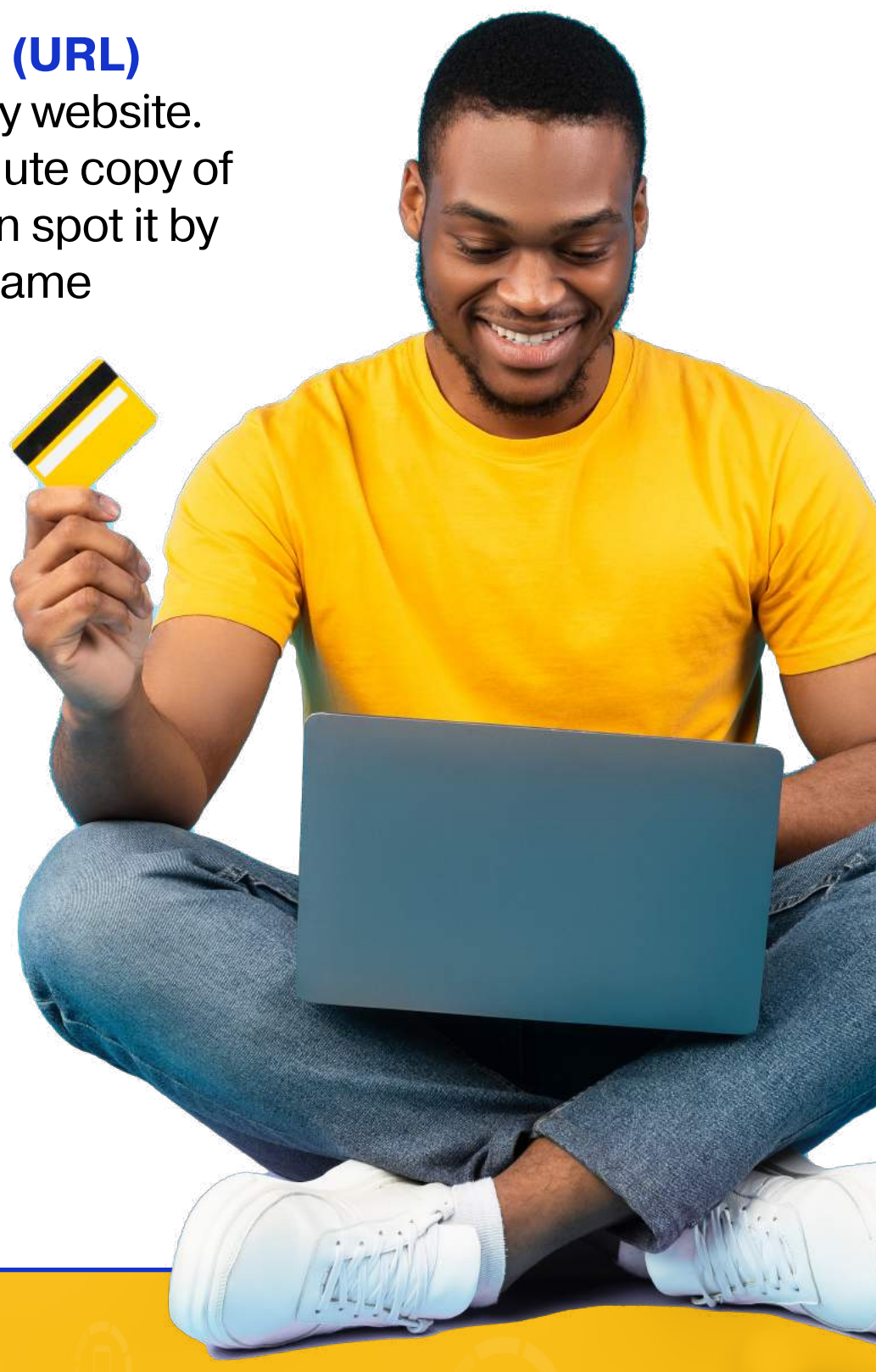
Verify the logo against that of the company or the bank's online page

Verify the full website name (URL) when navigating from third party website. Fraudsters may create an absolute copy of well-known website and you can spot it by verifying carefully the website name

Look out for pixelated and low-resolution images

Pay attention to the company name and the amount being authorized

Check for a lock icon next to the website link when you are making a payment



YOU ARE YOUR FIRST LINE OF DEFENSE

NEVER REVEAL sensitive information over the phone or through texts, especially:

- x Your account number
- x Your three-digit security code (CVV2) on the back of your card
- x Your one-time passwords

DO NOT CLICK on any links or download files you suspect are offering something too good to be true

DO NOT TRANSFER money to any strangers that approach you online asking for money

VISA