2023 seasonal scams

Fake ads on social media and webpages

The scammer uses name brands and deals too good to be true to lure shoppers to click a fake ad that can download malicious software onto your device and collect your credentials and payment card information on a fake merchant website.

What you can do

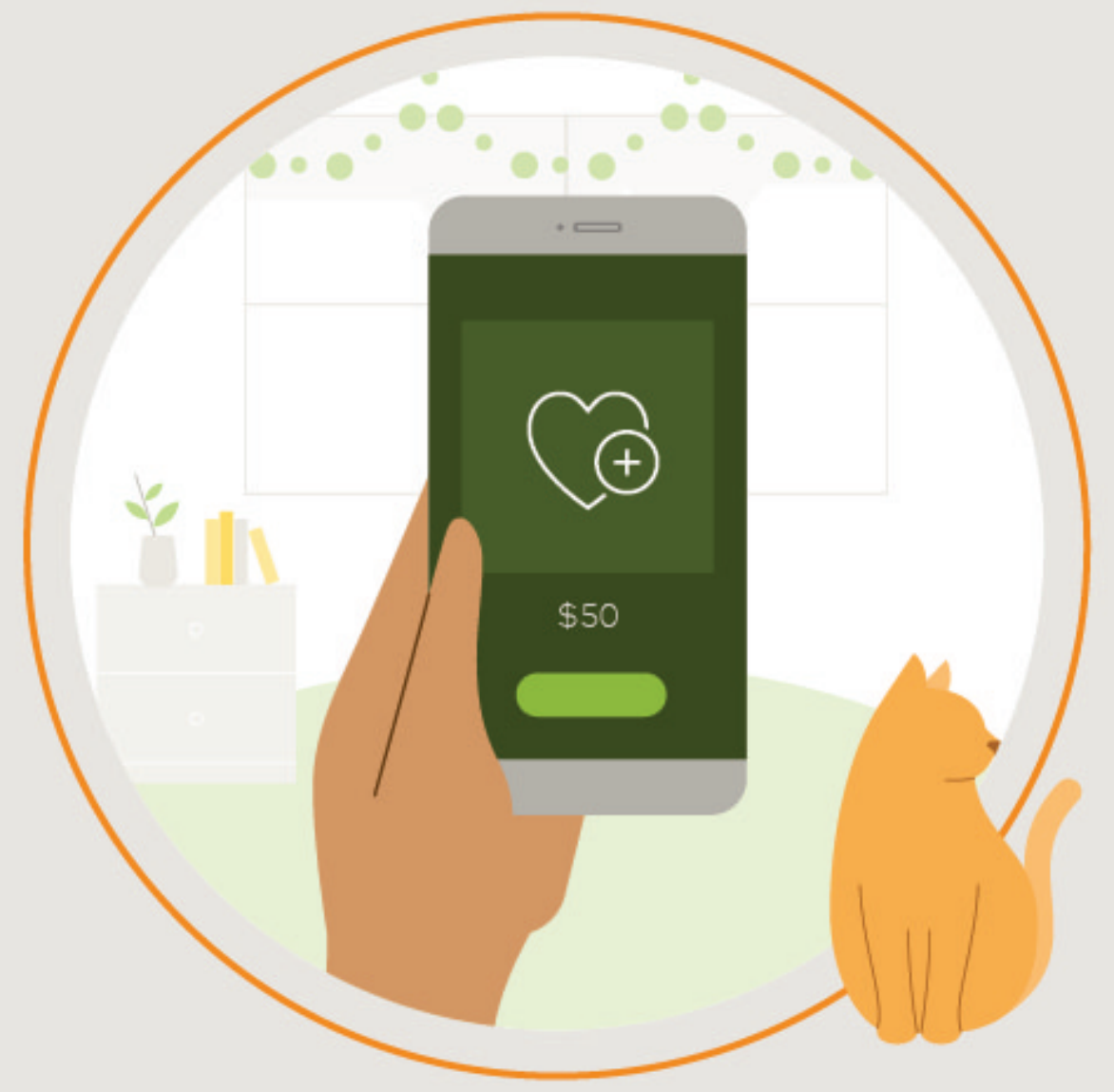
- Avoid clicking tempting website ads and visit the merchant's site directly.
- Conduct an online search to read reviews and validate the merchant has an address and return policy listed on their site.
- Think S for security and validate the retailer's website URL starts with "https," which adds additional security measures.
- Use a designated credit card that offers protection from fraudulent charges and monitor that account closely.

Social engineering scams

Social engineering scams appear in many forms such as phishing emails, smishing SMS text messages, vishing phone calls and QR code quishing. The scammer uses money saving offers, a sense of urgency and notices about your account, order or shipping as a lure to trigger shoppers to take the bait.

What you can do

- Visit the merchant's site directly and avoid clicking on links or opening an attachment on an account, order or shipping notice.
- Create a designated email account that is used for online shopping.
- Establish a unique long passphrase for each account and always enable multifactor authentication if offered. Password managers can help manage this process.
- Avoid engaging with QR codes in public spaces or sent in an email. Instead, visit the merchant's site directly.



Charity scams

The scammer preys on our goodwill during the holiday season by sending requests that appear legitimate but are actually for a fake charity.

What you can do

- Research the charity online using a reputable charity checker to ensure the organization is legitimate.
- Never provide payment information in response to a mailer, phone call, text message or email request. Instead, visit the charity's site directly.

What to do if you've been scammed

- Contact your financial institution to report the fraudulent activity.
- Reset all your passwords and maximize account security using your system settings. Create a long and strong unique passphrase with a variety of upper and lowercase letters, numbers and symbols that does not include self-identifying information that is publicly available on social media, like your pet's name.
- Report the incident to the authorities by searching for your country's national fraud and cybercrime reporting center.