factis®

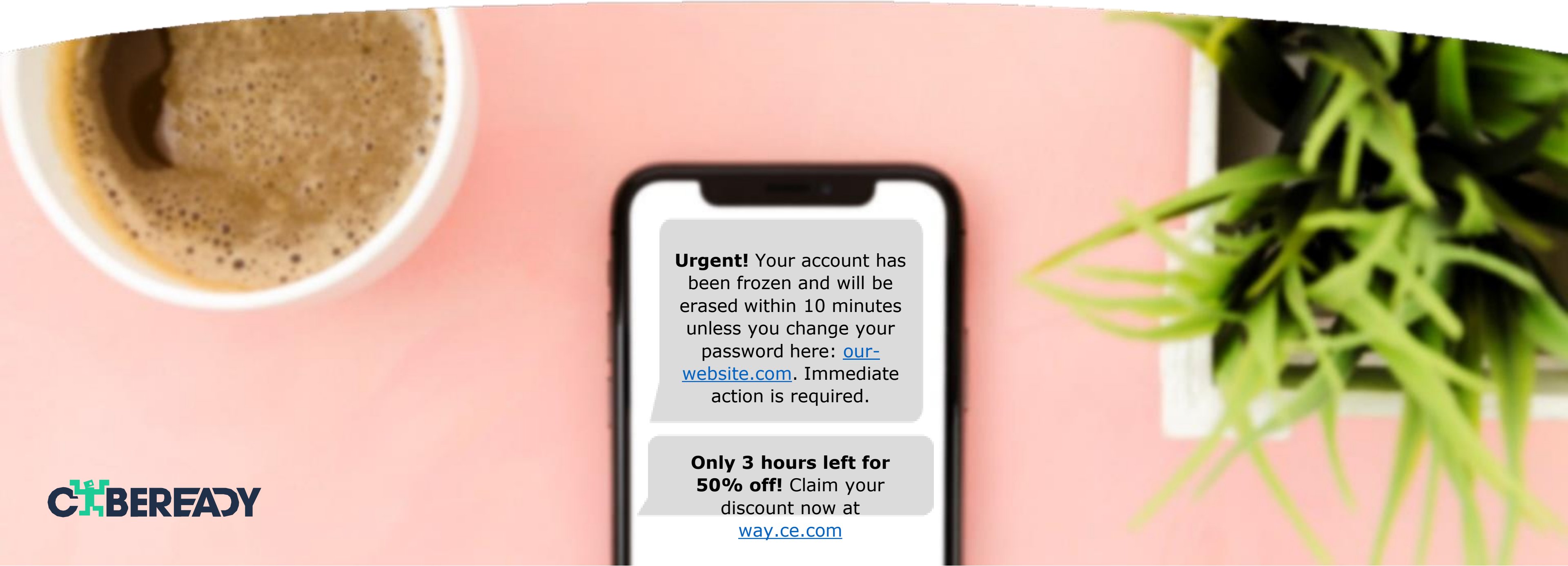
Protect yourself from smishing

CYBEREADY

‘Smishing’ is phishing that uses messaging to entice people to send money, passwords, or personal and financial information.

Smishing can occur on all messaging platforms (not just SMS) like WhatsApp, WeChat, social media DMs, etc.

Most smishing attempts will include an **urgent deadline, a threat, or an appealing offer** to encourage recipients to act quickly.



Urgent! Your account has been frozen and will be erased within 10 minutes unless you change your password here: our-website.com. Immediate action is required.

Only 3 hours left for 50% off! Claim your discount now at way.ce.com

Some messages will contain **malicious attachments or links,**

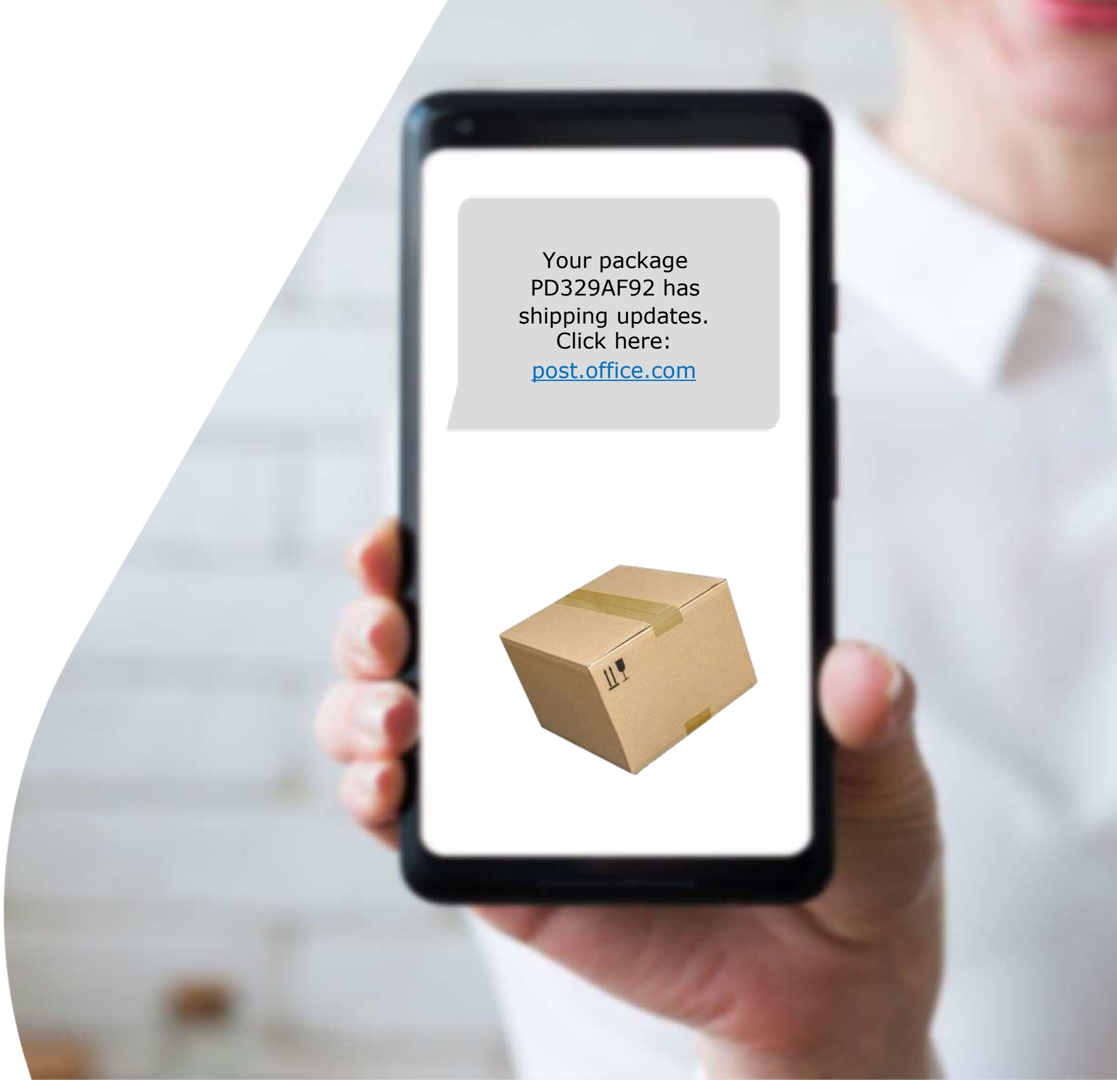
while others will ask the recipient to **reply directly** with personal information.

factis®

Typical smishing attacks include:

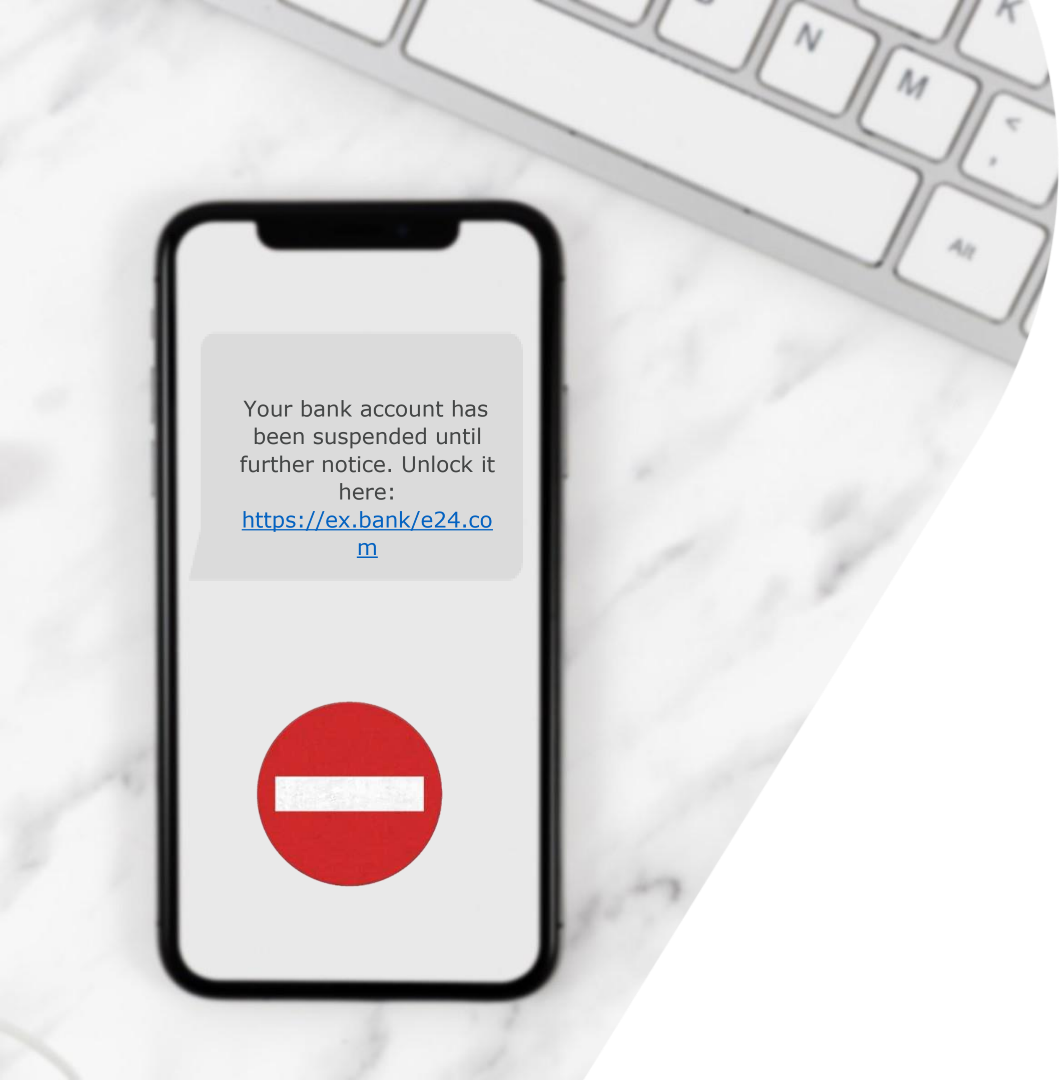
#1:

Fake package notifications that mimic real mail-order messages exploit our online shopping habits and desire to track deliveries.



Your package PD329AF92 has shipping updates. Click here: post.office.com

CYBEREADY



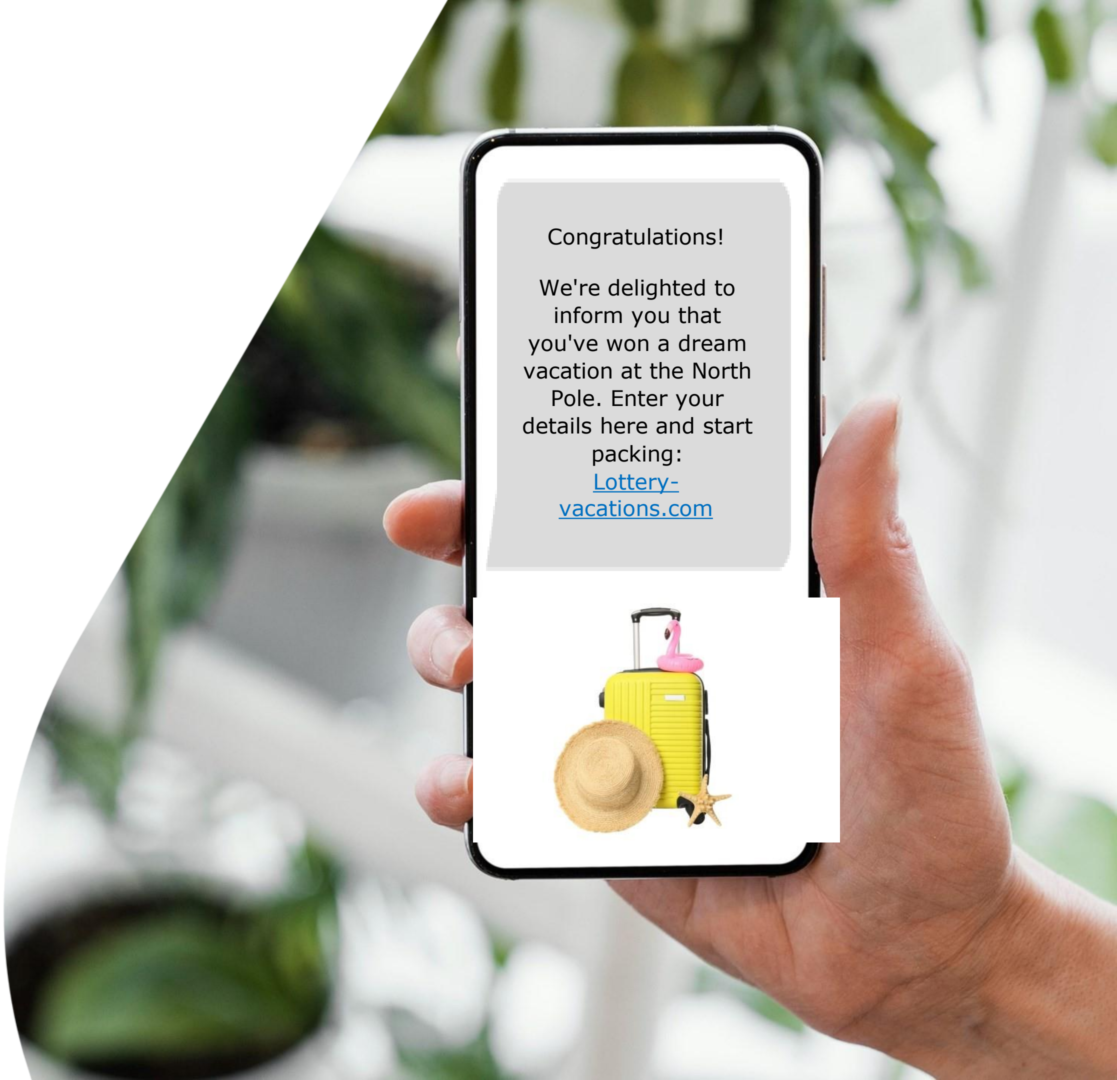
Your bank account has been suspended until further notice. Unlock it here: https://ex.bank/e24.com

#2:

Bogus notifications about account activity. Messages like these can be extremely stressful, prompting people to react hastily and carelessly.

#3:

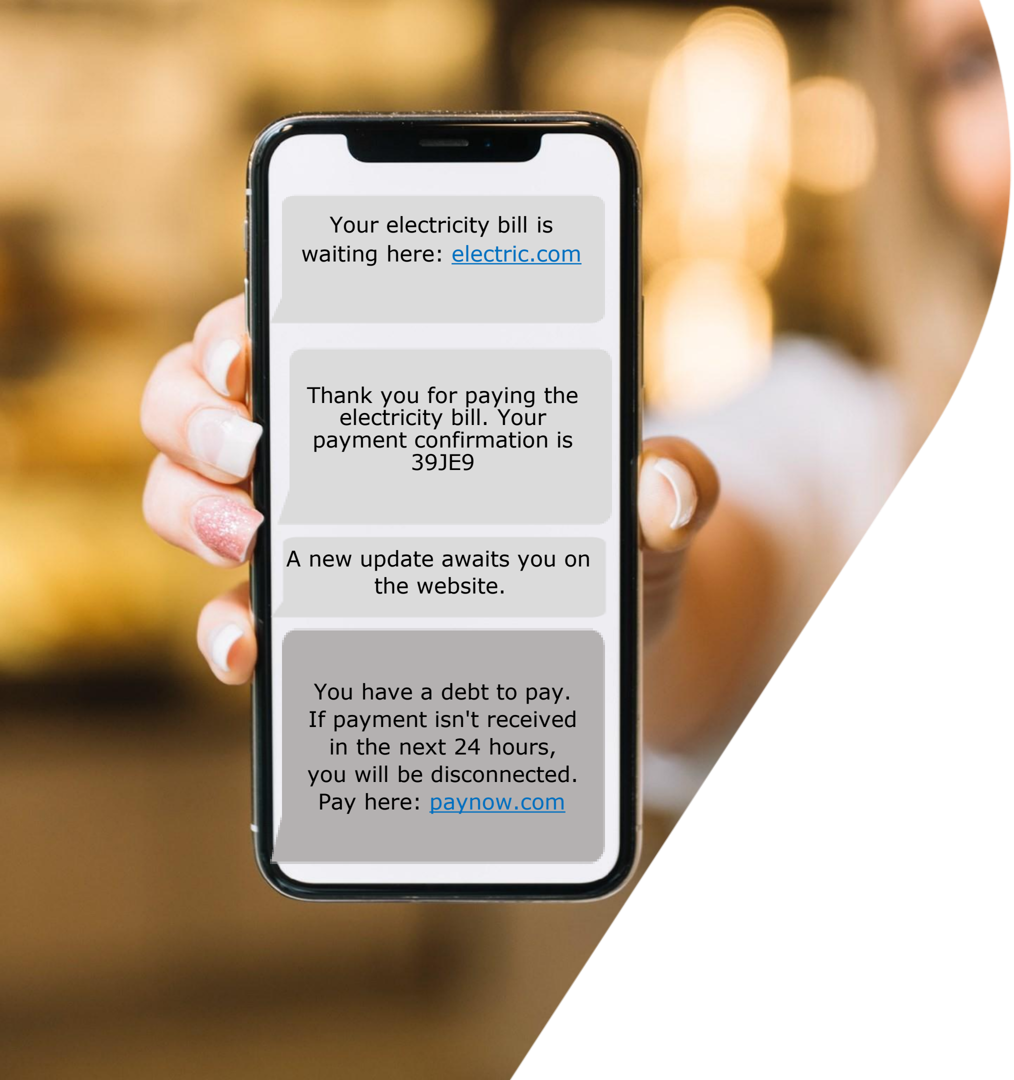
Messages that inform recipients of a prize. In their excitement, people often fail to realize the absurdity of winning a contest or sweepstakes they never entered.



Congratulations!

We're delighted to inform you that you've won a dream vacation at the North Pole. Enter your details here and start packing: Lottery-vacations.com

factis®



Your electricity bill is waiting here: electric.com

Thank you for paying the electricity bill. Your payment confirmation is 39JE9

A new update awaits you on the website.

You have a debt to pay. If payment isn't received in the next 24 hours, you will be disconnected. Pay here: paynow.com

Pay attention:

Received a new message in a recognized, existing thread? It's not necessarily trustworthy!

Hackers can insert malicious messages into earlier conversations so they appear to come from the same legitimate source.

CYBEREADY

What makes us vulnerable to smishing?

- Many of us mistakenly believe that text messages are more secure than other forms of communication.
- We're accustomed to receiving many messages a day from unknown numbers.
- Mobile devices have small displays, which makes it harder to pay attention to minor details.

What can you do?

Consider any text messages with links or attachments to be unsafe
and avoid clicking on them.

"Unsubscribe" buttons can also contain malicious links
Don’t click on them, either.

Don’t respond to messages from unknown numbers
no matter how innocent they seem.

Keep an eye out for persuasive wording
like "urgent update" and "limited time offer," as these are designed to entice you to click quickly.

Received a message from your bank, or credit card company?

Check if the information is displayed on the website or mobile app.

Or

Contact a company representative.

*Don't use any links or numbers provided within the message.

Got a package delivery notification?

If the company is well known:

Without clicking on any message links, browse the company's website and enter the package number there.

Check if the details match a product you ordered, and if so, you can enter the link in the message.

If the package details aren’t found, the message is probably a scam.

If you’re unfamiliar with the delivery company:

- Use social media to gauge the company's credibility.
- If you can’t find any proof of its reliability, ignore the message.

Remember:

If something seems off, it's best not to click or respond.
Malicious messages cannot cause you harm if you simply **ignore** them.