KeepUp ACADEMY

10 Scam Messages You Should Never Click

A plain-language safety guide for texts, emails, online alerts, and suspicious requests.

The KeepUp Academy rule:

Pause before you click. If a message creates pressure, asks for money, asks for a code, or sends you to a link, slow down and verify it another way.

Use this guide for yourself, or share it with a parent, grandparent, friend, or loved one who wants to feel safer online.

Educational resource only. If you think money or personal information was stolen, contact your bank, account provider, or appropriate authorities directly.

How to Use This Guide

Scam messages often work because they look familiar, sound urgent, or make you feel like you need to act right away. This guide helps you recognize common patterns and choose a safer next step.

- ✓ Read the example message first. Notice how it tries to create urgency or curiosity.
- ✓ Review why the message is suspicious. Scammers often reuse the same patterns.
- ✓ Do not click links, call numbers, reply, send money, or share security codes from suspicious messages.
- ✓ Verify through the official app, official website, or a known phone number you already trust.
- ✓ When unsure, ask a trusted person to review the message with you before acting.

Quick rule of thumb

If the message asks you to rush, pay, click, download, call a strange number, or share a code, treat it as suspicious until you verify it another way.

Official reporting reminders

The FTC recommends reporting scam texts by forwarding them to 7726 (SPAM), reporting phishing attempts to ReportFraud.ftc.gov, and forwarding phishing emails to reportphishing@apwg.org. These reporting steps help providers and agencies spot scam patterns.

Scam Message 1

Fake Delivery Text

Example message

“Your package could not be delivered. Confirm your address and pay a small redelivery fee here: [link]”

Why it is suspicious	What not to do	What to do instead
It creates urgency around a package and asks you to click a link or pay a fee. The link may lead to a fake delivery page designed to collect payment or personal details.	Do not click the link, enter card information, or reply with your address.	Open the delivery company’s official app or website yourself. Use the tracking number from your original order confirmation, not the suspicious text.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 2

Fake Bank Alert

Example message

“Your bank account has been locked due to suspicious activity. Verify your login immediately: [link]”

Why it is suspicious	What not to do	What to do instead
It uses fear to push you into clicking quickly. The link may lead to a fake login page that steals your username and password.	Do not click the link or enter your login information from the message.	Open your banking app directly or type the bank’s official website yourself. Call the number on the back of your card if you are concerned.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 3

Security Code Request

Example message

“This is support. We sent you a six-digit code. Read it back to confirm your account.”

Why it is suspicious	What not to do	What to do instead
A security code can let someone access or reset your account. Scammers may pretend to be support so they can use the code before it expires.	Do not share verification codes, one-time passwords, or two-factor authentication codes with someone who contacted you.	End the conversation. Go to the official app or website and change your password if you believe the request was suspicious.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 4

Gift Card Payment Scam

Example message

“You owe a balance. Buy gift cards and send us the numbers today to avoid a penalty.”

Why it is suspicious	What not to do	What to do instead
Legitimate companies, government agencies, and banks generally do not ask for payment through gift cards. Gift card numbers are like cash once shared.	Do not buy gift cards, scratch off codes, photograph cards, or send card numbers.	Stop communicating. Call the organization using a known official number and ask whether any balance is actually owed.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 5

Fake Tech Support Pop-Up

Example message

“Your computer is infected. Call Microsoft/Apple Support now at this number.”

Why it is suspicious	What not to do	What to do instead
Scary pop-ups often pretend to be official support. The goal may be to get you to call, pay, or install remote access software.	Do not call the number on the pop-up, download software, or give remote access to your device.	Close the browser window. Restart the device if needed. Contact official support through the company’s real website or a trusted local support option.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 6

Prize or Free Gift Scam

Example message

“Congratulations! You won a free phone. Pay shipping to claim your prize.”

Why it is suspicious	What not to do	What to do instead
The message creates excitement and asks for a small payment or personal details. The “free” prize may be a trick to collect payment information.	Do not pay shipping, enter card information, or share personal details for an unexpected prize.	Ignore the message. If it claims to be from a company you use, go directly to that company’s official website to verify.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 7

Fake Subscription Renewal

Example message

“Your antivirus subscription renewed for $399. Call this number within 24 hours to cancel.”

Why it is suspicious	What not to do	What to do instead
The message may scare you with a large charge and push you to call a fake support number. The scammer may ask for bank details or remote access.	Do not call the number in the message or allow remote access to your device.	Check your real bank or credit card activity directly. Contact the company through its official website if you have a real subscription.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 8

Social Media Friend Scam

Example message

“Hi, it’s me. I lost my phone. Can you send money or a code to help me get back in?”

Why it is suspicious	What not to do	What to do instead
Scammers may use hacked or fake profiles to pretend to be someone you know. They often ask for money, codes, or urgent help.	Do not send money, gift cards, payment app transfers, or verification codes based only on a message.	Contact the person another way, such as calling their known phone number or asking a family member to confirm.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 9

Fake Government or Traffic Notice

Example message

“You have an unpaid toll, ticket, or government fee. Pay now to avoid additional penalties: [link]”

Why it is suspicious	What not to do	What to do instead
The message uses official-sounding language and pressure. It may link to a fake payment page or ask for personal information.	Do not click the link or enter payment details from the text.	Visit the official government, toll, or agency website directly. Search carefully or use a known bill/notice you already received.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Scam Message 10

Payment App Request

Example message

“I accidentally sent you money. Please send it back through this payment app.”

Why it is suspicious	What not to do	What to do instead
Scammers may use fake screenshots or stolen accounts to pressure you into sending money. Some payment transfers are hard to reverse.	Do not send money back based only on a message or screenshot.	Open the payment app directly and review your account activity. Contact the app’s official support if you are unsure.

Simple safety reminder

Do not use the link, phone number, or reply option inside a suspicious message. Go to the official app, official website, or a known phone number instead.

Before You Click: A Simple Safety Checklist

Use this checklist whenever a text, email, call, pop-up, or social media message asks you to do something quickly.

Question	Why it matters
Does the message create urgency?	Examples: “Act now,” “your account will close,” “pay today,” or “verify immediately.”
Is the sender unfamiliar or slightly odd?	Check for misspellings, strange email addresses, unknown numbers, or links that do not match the official company.
Does it ask for money, gift cards, payment app transfers, or cryptocurrency?	Treat unusual payment methods as a major warning sign.
Does it ask for a security code?	Never share one-time codes with someone who contacted you.
Does the link look suspicious?	Do not click shortened, strange, or misspelled links.
Can you verify it another way?	Use the official app, website, statement, card number, or a known phone number.
Would pausing help?	If you feel rushed or scared, step away and ask someone you trust.

Best habit

Go directly to the official source. Do not use the link, phone number, or reply option inside a message you did not expect.

What To Do If You Already Clicked

Clicking a link does not always mean something bad happened. The next step depends on what you did after clicking.

If you...	Do this next
Clicked but did not enter information	Close the page. Do not download anything. Do not keep clicking. If you are unsure, ask a trusted person to review the message.
Entered a password	Go to the official website or app directly and change the password. Use a different password if the same one is used elsewhere. Turn on two-step verification if available.
Entered card or bank information	Contact your bank or card company immediately using the number on the back of your card or the official app. Watch for unfamiliar transactions.
Shared a security code	Go to the official account directly, change the password, review account activity, and contact the company if you see anything unfamiliar.
Downloaded something	Stop using the download. Consider disconnecting from the internet and asking trusted technical support to check the device.
Sent money or gift card numbers	Contact the payment provider, bank, or gift card company right away. Report the scam and ask whether the transaction can be stopped or reversed.

Report it

In the United States, you can report scams and phishing attempts to the FTC at ReportFraud.ftc.gov. You can also forward scam text messages to 7726 (SPAM).

Keep Learning With KeepUp Academy

This guide is one small step toward safer everyday technology habits. KeepUp Academy is being built to help adults learn with short lessons, printable guides, scam alerts, and simple learning paths.

What to learn next

Start with online safety basics, then build confidence with smartphones, email, video calls, passwords, online shopping, and digital payments.

Visit KeepUp Academy to continue building safer, more confident digital habits.

Sources consulted for reporting guidance: Federal Trade Commission consumer guidance on phishing, spam texts, and ReportFraud.ftc.gov. This guide is educational and does not replace official, financial, legal, or technical support.