
RESOURCE 08 | DON'T CLICK YET COMPANION RESOURCE

Scam Response Scripts

Companion resource for Don't Click Yet. Referenced on page 202.

Purpose: Use ready-to-adapt phrases for slowing down pressure, verifying requests, and responding safely.

Storage reminder: If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

Scams work best when you are forced to improvise under pressure. A script gives you words before you need them.

You do not need to sound clever, rude, technical, or suspicious. You only need to slow the situation down and move the conversation to a safer path.

Use these scripts when a message, call, email, pop-up, or money request feels urgent, confusing, emotional, or unusual.

How to Use These Scripts

You can copy these scripts exactly or adjust them to sound more natural. The goal is not to win an argument with a scammer. The goal is to stop following the path they are trying to create.

A good response usually does one of three things:

- It pauses the interaction.
- It verifies through another route.
- It ends the conversation.

You do not owe an unexpected caller, message sender, or pop-up a long explanation.

The Basic Pause Script

Use this whenever something feels urgent, unusual, or emotionally intense.

"I do not make decisions like this immediately. I am going to stop here and verify through another route."

Alternative versions:

"I need to check this independently before I do anything."

"I do not handle money, codes, or account changes through unexpected messages."

"I am going to call back using a number I already know is official."

"I will not continue this conversation until I verify who I am speaking with."

If a Bank Text or Email Arrives

Use this when a message claims your bank account is locked, suspicious activity was detected, or a transaction needs review.

Do not click the link in the message.

Script to yourself:

"I will not use this link. I will open the bank app directly or call the number on my card."

If replying is necessary, keep it simple:

"I will contact the bank directly."

If someone calls claiming to be from the bank:

"I am not comfortable continuing this call. I will call the bank using the number on my card."

If the caller pressures you:

"That pressure is exactly why I am ending the call. I will contact the bank directly."

If Someone Asks for a Verification Code

Use this when a caller, texter, or email asks you to read, forward, type, or approve a code.

"I do not share verification codes with anyone who contacts me."

Alternative versions:

"If I did not start this sign-in, I will not provide the code."

"I will not approve a login I did not request."

"I am going to stop and check the account directly."

"If this is legitimate, I can handle it through the official app or website."

If the person says they cannot help without the code:

"Then I will contact the company directly through a trusted number."

If a Family Member Asks for Urgent Money

Use this when a message appears to come from a child, grandchild, spouse, sibling, friend, or relative asking for money or secrecy.

"I want to help, but I need to verify first. What is our family phrase?"

Alternative versions:

"You know our rule. What is the phrase?"

"I will not send money until I confirm this another way."

"I am going to call you on your regular number."

"If this is really an emergency, verification will help us respond correctly."

If the person says not to tell anyone:

“That is not our family rule. We verify urgent requests.”

If the person pressures harder:

“I am stopping here and calling another family member.”

If Someone Says Not to Tell Anyone

Secrecy is a common warning sign, especially in family, romance, financial, and emergency scams.

“I do not keep urgent money requests secret.”

Alternative versions:

“If this is real, another trusted person can help us.”

“I will not send money while being told to stay silent.”

“I am going to involve someone I trust before doing anything.”

“Secrecy makes this feel unsafe, so I am stopping.”

If Someone Requests Gift Cards

Gift cards are a major warning sign when requested for emergencies, bills, taxes, support, refunds, prizes, romance, or account problems.

“I do not pay people or solve account problems with gift cards.”

Alternative versions:

“No legitimate bank, agency, employer, utility, or support department needs gift card numbers.”

“I will not buy gift cards or read the numbers to anyone.”

“I am ending this conversation and verifying directly.”

If you already bought gift cards but have not shared the numbers:

“I will not share the card numbers. I am going to contact the store or card issuer for guidance.”

If Someone Requests Cryptocurrency, Wire Transfer, or Payment App Transfer

Use this when someone pressures you to send money quickly through a method that may be hard to reverse.

“I do not send fast payments under pressure.”

Alternative versions:

“I need to verify this independently before any money moves.”

“I will not send money to a third party I do not know.”

“I do not use cryptocurrency, wire transfers, or payment apps for urgent requests from unexpected messages.”

“If this is legitimate, it can wait while I verify.”

If a Computer Pop-Up Says You Are Infected

Use this when a warning appears on your screen telling you to call a number, not shut down, or act immediately.

Do not call the number on the pop-up.

Script to yourself:

“I will not call the number on this screen. I will close the page or shut down the computer and ask a trusted person for help.”

If the pop-up will not close:

“I will stop using the browser and restart the computer if needed.”

If you are unsure what to do:

“I will take a photo of the screen and ask for help before clicking anything else.”

If Someone Asks for Remote Access

Use this when a caller, message, website, or pop-up asks you to install software or allow screen control.

“I do not allow remote access unless I started the support request through a trusted channel.”

Alternative versions:

“I will not install remote access software because of an unexpected call or warning.”

“I am ending this session and contacting support directly.”

“I need to verify this with someone I trust before allowing access.”

If the person says your computer will be damaged if you disconnect:

“I am still ending the session. I will get trusted help.”

If You Are Already on a Call and Feel Unsure

Use this when you are in the middle of a conversation and something starts to feel wrong.

“I need to stop and verify this.”

Alternative versions:

“I am not comfortable continuing.”

“I do not make financial or account decisions while on an unexpected call.”

“I am going to hang up and contact the company directly.”

“I will call back through an official number.”

Then hang up.

You do not need permission to end the call.

If the Caller Becomes Angry or Threatening

Pressure, anger, threats, and intimidation are warning signs.

“I will not continue while being pressured.”

Alternative versions:

“Threats do not make this legitimate. I am ending the call.”

“I am going to verify this independently.”

“I will contact the company, bank, or agency directly.”

“I do not respond to threats over the phone.”

Then end the conversation.

If the Caller Claims to Be the Government

Use this when someone claims to be from the IRS, Social Security, immigration, Medicare, law enforcement, a court, or another government office and demands immediate action.

“I do not provide information or payment during unexpected calls. I will contact the agency directly.”

Alternative versions:

“I will not pay by gift card, cryptocurrency, wire transfer, or payment app.”

“I need written information through official channels.”

“I will verify this using an official government website or phone number.”

“I am ending this call now.”

If the Message Claims a Delivery Problem

Use this when a delivery text or email says a package is delayed, an address is incomplete, or a small fee is needed.

“I will not use this link. I will check the order or delivery through the official store or carrier website.”

Alternative versions:

“I will open the app directly.”

“I will type the website myself.”

“I will not enter payment information through a delivery text.”

If a Marketplace Buyer or Seller Pressures You

Use this when buying or selling through online marketplaces.

“I only communicate and pay through the official platform.”

Alternative versions:

“I will not move this conversation to another app.”

“I will not accept overpayment and send money back.”

“I will not pay a deposit outside the platform.”

“I will meet only in a safe agreed location and will not rush.”

“If this is too urgent, I am not comfortable continuing.”

If a Friend Sends a Strange Link

Use this when a link appears to come from someone you know but feels unusual.

“Did you mean to send this?”

Alternative versions:

“I am checking before I click. Is this really from you?”

“This looks unusual. Can you confirm what it is?”

“I will not open it until I hear from you directly.”

If the friend did not send it:

"Your account may be sending suspicious messages. You may want to change your password and check your account security."

If You Clicked a Suspicious Link

Use this to explain what happened when asking for help.

"I clicked a link that may have been suspicious. I did not enter any information."

Or:

"I clicked a link and entered my username and password."

Or:

"I clicked a link and entered payment information."

Or:

"I clicked a link and downloaded something."

Then say:

"I need help deciding what to do next."

The details matter. Be honest about what happened after the click.

If You Shared a Password

Use this with a trusted person, bank, company, or support contact.

"I may have shared my password on a fake website or with someone I do not trust. I need to secure the account."

Helpful details to include:

- Which account was involved
- When it happened
- Whether the password was used anywhere else
- Whether MFA was turned on
- Whether you saw any unusual activity
- Whether you still have access to the account

Script to yourself:

"I need to change this password from a trusted device and change it anywhere else I reused it."

If You Shared a Code

Use this when asking for help after sharing a verification code.

"I shared a verification code with someone who contacted me unexpectedly. I need to check the account connected to that code."

Helpful details to include:

- Which company sent the code
- Whether you know what action the code approved
- Whether you shared it by phone, text, email, or website
- Whether you still have access to the account
- Whether you see any unusual activity

Script to yourself:

“A real code can still be part of a fake request. I need to review the account now.”

If You Sent Money

Use this with a bank, card issuer, payment app, or trusted helper.

“I believe I was tricked into sending money. I need to report it and prevent further loss.”

Helpful details to include:

- Date and time
- Amount
- Payment method
- Recipient name, username, phone number, email, or wallet address
- Reason you were given
- Screenshots or receipts
- Whether the person is still contacting you

Questions to ask the bank or payment service:

- Can this transaction be stopped, reversed, or disputed?
- Should my card or account be locked?
- Should I replace the card?
- Do I need a case number?
- What evidence should I save?
- Should I watch for additional charges?

If You Allowed Remote Access

Use this when asking for help after someone viewed or controlled your computer or phone.

“I allowed someone remote access to my device, and I now believe it may have been a scam.”

Helpful details to include:

- When it happened
- How long the access lasted
- What program or tool was used, if known
- Whether you typed passwords during the session
- Whether you opened banking, email, or sensitive files
- Whether you paid money
- Whether the person called back
- Whether the device is still connected to the internet

Script to yourself:

"I should stop using this device for sensitive activity until it is reviewed."

If You Need to Tell a Family Member

Use this when you feel embarrassed but need help.

"I need to tell you something, and I need you not to judge me first. I may have been scammed, and I need help limiting the damage."

Alternative versions:

"I clicked something and I am not sure what to do next."

"I sent money and now I think it may have been a scam."

"I gave someone remote access to my computer."

"I shared a code and I need help checking the account."

"I am embarrassed, but I know it is better to ask for help now."

If You Are Helping Someone Else

Use calm language first.

"Thank you for telling me. We can deal with this."

Alternative versions:

"You did the right thing by saying something."

"Let's focus first on stopping more damage."

"We can ask questions without blaming you."

"Do not delete anything yet. The messages may help."

"Let's write down what happened while it is fresh."

Avoid saying:

- "How could you fall for that?"
- "I told you not to click things."
- "That was obviously fake."
- "You should have known better."
- "Give me your phone; I'll handle everything."

Shame makes people hide. Calm help makes recovery easier.

If You Need to Contact a Bank or Card Issuer

Use this script when calling through the number on your card or official app.

"Hello, I believe I may have been targeted by a scam. I want to protect my account and report possible fraud."

Then explain:

"I made a payment / shared information / entered my card details / noticed a suspicious transaction."

Ask:

- "Can you check for suspicious activity?"
- "Should the card be locked or replaced?"
- "Can the transaction be disputed or stopped?"
- "Is there a case number?"
- "What documentation should I keep?"
- "Are there additional steps I should take?"

Write down:

- Date and time of call
- Name or ID of representative, if provided
- Case number
- Next steps
- Any promised follow-up

If You Need to Contact a Company Being Impersonated

Use this when reporting a fake message, website, call, or email.

"I received a message or call from someone claiming to represent your company. I believe it may be fraudulent and would like to report it."

Include:

- Sender email or phone number
- Website link, if safe to copy
- Screenshot
- Date and time
- What they asked you to do
- Whether you shared information or paid money

Do not use contact details from the suspicious message. Use the company's official website, app, bill, statement, or trusted support channel.

If You Need to Report Identity Theft

Use this when sensitive personal information may have been misused.

"I believe my personal information may have been used without permission. I need to document this and begin recovery steps."

Write down:

- What information may have been exposed
- How you discovered the problem
- Any accounts opened or changed
- Any credit inquiries or bills you do not recognize
- Any letters, emails, calls, or notices received
- Dates and case numbers
- Institutions contacted

Identity theft may require more than changing passwords. Use official recovery guidance and keep records of every step.

If You Need Time to Think

You can use this script in many situations.

“I am not refusing to deal with this. I am refusing to rush.”

Alternative versions:

“If this is real, it can wait while I verify.”

“I will not make this decision while I feel pressured.”

“I need to involve someone I trust.”

“I will continue only through an official channel.”

If You Want to Warn Family or Friends

Use this after a scam attempt or near miss.

“I want to let you know about something that happened so you can watch for it too.”

Then explain briefly:

“I received a message pretending to be from the bank.”

Or:

“Someone pretended to be a family member asking for money.”

Or:

“A fake computer warning told me to call support.”

Then add:

“No one should feel embarrassed if this happens. The important thing is to stop, verify, and ask for help early.”

Personal Scripts

Write your own versions of the most important scripts below.

My pause script:

My bank verification script:

My family money request script:

My verification code script:

My remote access script:

My ask-for-help script:

Final Reminder

You do not need to argue with a scammer.

You do not need to prove they are fake.

You do not need to be polite while being pressured.

Pause.

End the conversation.

Choose your own route.

Ask for help early.