How to Recognize Scam Emails and Texts

A Click Giraffe Guide for Everyday Digital Safety

Scam emails and texts are designed to make you react quickly.

They may look like they come from a bank, delivery company, government agency, technology company, online store, payment app, employer, friend, or family member.

The goal is usually simple:

- Make you click a link.
- Make you open an attachment.
- Make you share a password.
- Make you share a verification code.
- Make you send money.
- Make you install software.
- Make you give remote access to your device.
- Make you panic before you think.

This guide will help you slow down, recognize common warning signs, and decide what to do next.

The Most Important Rule

Urgency is the warning sign.

Scammers often want you to feel afraid, rushed, embarrassed, or excited.

They may say:

- Your account will be locked.
- Your package cannot be delivered.
- Your bank account is at risk.
- Your computer is infected.
- You owe money.
- You won a prize.
- Your child or grandchild is in trouble.
- You must verify your identity immediately.
- You must not tell anyone.
- You need to send money right now.

- You need to call this number immediately.
- You need to click this link before time runs out.

When a message makes you feel rushed, stop.

Do not click immediately.
Do not reply immediately.
Do not call the number in the message.
Do not share codes.
Do not send money.

Pause and verify.

Common Scam Message Types

1. Fake Account Alert

These messages claim that an account has been locked, suspended, accessed from a new device, or scheduled for deletion.

They may pretend to come from:

- Google
- Microsoft
- Apple
- Amazon
- PayPal
- Facebook
- Instagram
- Netflix
- Your bank
- Your phone carrier

Warning signs

[ ] The message says your account will be locked immediately.
[ ] The link goes to a strange-looking website.
[ ] The message asks you to verify your password.
[ ] The message asks for a code sent to your phone.
[ ] The message contains spelling or formatting mistakes.
[ ] The sender address looks unusual.
[ ] The message creates panic.

Safer action

Do not click the link in the message.

Instead, open the official app or type the official website address yourself. Check your account from there.

---

2. Fake Package Delivery Text

These messages say a package cannot be delivered, shipping information is missing, or a small fee is required.

They may pretend to come from:

- USPS
- UPS
- FedEx
- DHL
- Amazon
- Other delivery services

Warning signs

[ ] You were not expecting a package.
[ ] The link is shortened or strange.
[ ] The message asks for a small payment.
[ ] The message asks for your card number.
[ ] The message uses urgent language.
[ ] The message came from a random phone number or email address.

Safer action

Do not use the link in the text.

Go directly to the delivery company’s website or app and enter your tracking number if you have one.

---

3. Fake Bank or Payment App Alert

These messages claim there is suspicious activity, a failed payment, a frozen account, or a transfer that needs approval.

They may pretend to come from:

- Your bank
- Zelle
- Venmo
- Cash App
- PayPal
- Apple Pay
- Google Pay
- Credit card companies

Warning signs

[ ] The message asks you to click a link to “secure” your account.
[ ] The message asks for your password.
[ ] The message asks for a one-time code.
[ ] The message tells you to move money to “protect” it.
[ ] The message tells you not to tell anyone.
[ ] The message asks you to call a number provided in the message.

Safer action

Open your banking app directly or call the number on the back of your card.

Never call the number inside the suspicious message.

---

4. Fake Tech Support Message

These scams may appear as emails, pop-ups, phone calls, or text messages.

They may claim:

- Your computer is infected.
- Your files are at risk.
- Your Microsoft account is compromised.
- Your Apple account is locked.
- You must call support immediately.
- You need to install remote-access software.

Warning signs

[ ] A pop-up tells you to call a phone number.
[ ] Someone says they are from Microsoft, Apple, Google, or your antivirus company and called

you unexpectedly.
[ ] Someone asks for remote access to your computer.
[ ] Someone asks you to install AnyDesk, TeamViewer, UltraViewer, or similar software unexpectedly.
[ ] Someone asks you to pay with gift cards, cryptocurrency, wire transfer, or payment apps.
[ ] Someone asks you to log into your bank while they are connected to your computer.

Safer action

Do not call the number in the pop-up.

Do not give remote access.

If you are worried, turn off the device and ask a trusted person or qualified professional for help.

---

5. Fake Family Emergency

These scams claim a family member is in trouble.

The message may say:

- A grandchild was arrested.
- A child had an accident.
- A relative lost their phone.
- A family member needs urgent money.
- Someone is in the hospital.
- Someone is traveling and needs help.

Scammers may use names, social media details, or even voice impersonation.

Warning signs

[ ] The person asks for money urgently.
[ ] The person says not to tell anyone.
[ ] The message comes from a new number.
[ ] The voice or writing style feels slightly wrong.
[ ] The person refuses to answer basic family questions.
[ ] The payment method is unusual.

Safer action

Use a family verification phrase.

Call the person through a number you already know. If you cannot reach them, call another trusted family member before taking action.

---

6. Fake Invoice or Subscription Renewal

These scams claim you purchased something or that a subscription is renewing.

Common fake invoices may mention:

- Norton
- McAfee
- Geek Squad
- PayPal
- Amazon
- Apple
- Microsoft
- QuickBooks
- Antivirus renewals
- Computer protection plans

Warning signs

[ ] You do not recognize the purchase.
[ ] The message includes a phone number to cancel.
[ ] The amount is high enough to scare you.
[ ] The sender address looks strange.
[ ] The invoice is attached as a PDF or image.
[ ] The message tries to make you call quickly.

Safer action

Do not call the number in the invoice.

Check the official account directly. If no charge appears in your real account, the invoice may be fake.

---

7. Fake Prize, Refund, or Government Payment

These messages promise money or benefits.

They may claim:

- You won a prize.
- You are owed a refund.
- A government payment is waiting.
- You qualify for a grant.
- You must pay a small fee to receive money.
- You need to provide personal information.

Warning signs

[ ] You did not enter a contest.
[ ] You must pay money to receive money.
[ ] The message asks for bank details.
[ ] The message asks for your Social Security number.
[ ] The message asks for gift cards or cryptocurrency.
[ ] The message sounds too good to be true.

Safer action

Do not provide information through the message.

Verify directly through official websites or trusted phone numbers.

---

8. Fake Job, Client, or Freelancer Opportunity

Freelancers and remote workers are common targets.

The scam may involve:

- A fake job offer.
- A fake client.
- A fake check.
- A request to buy equipment.
- A request to receive and forward money.
- A suspicious file attachment.
- A link to a fake login page.

Warning signs

[ ] The offer is unusually generous.
[ ] The person wants to hire you without a proper conversation.
[ ] You receive a check and are asked to send part of the money elsewhere.
[ ] You are asked to buy equipment from a specific vendor.

[ ] The client sends files from strange links.
[ ] The communication moves quickly to payment or bank details.

Safer action

Verify the company independently.

Do not deposit suspicious checks or send money back to anyone. Be careful with files, links, and requests for personal information.

The 10-Second Scam Test

Before clicking, replying, calling, or paying, ask:

1. Was I expecting this message?
2. Does it create urgency or fear?
3. Is it asking for money, passwords, codes, or personal information?
4. Does the sender address or phone number look unusual?
5. Is the link strange, shortened, or misspelled?
6. Does the message ask me to keep it secret?
7. Is the payment method unusual?
8. Would the real company contact me this way?
9. Can I verify this through an official app, website, or known phone number?
10. Would I advise a family member to slow down before acting?

If the message fails this test, pause.

How to Check an Email Safely

Step 1: Look at the sender

Do not only look at the display name.

A message may say “Amazon Support” or “Microsoft Security,” but the real sender address may be unrelated.

Look for:

[ ] Misspelled domains.
[ ] Extra words or strange characters.
[ ] Free email addresses pretending to be companies.
[ ] Domains that look similar but are not exact.

Example:

- `support@amazon.com` may look normal.
- `support-amazon-security@example-mail.com` is suspicious.
- `amaz0n-security-login.com` is suspicious.

Step 2: Check the greeting

Scam messages often use generic greetings.

Examples:

- Dear customer
- Dear user
- Dear account holder
- Hello client

This alone does not prove a scam, but it is a warning sign.

Step 3: Look for pressure

Words like urgent, immediate, final warning, action required, account locked, legal action, or last chance are often used to rush you.

Step 4: Do not open unexpected attachments

Be careful with unexpected:

- PDFs
- Word documents
- Excel files
- ZIP files
- Invoices
- Receipts
- Voicemails
- Shipping documents

If you were not expecting the file, verify before opening it.

Step 5: Do not use the link

If the message says there is a problem with your account, go directly to the official website or app.

How to Check a Text Message Safely

Scam texts are often short, urgent, and link-based.

They may say:

- Your package is delayed.
- Your bank account is locked.
- Your payment failed.
- Your toll is unpaid.
- Your account needs verification.
- Your card was charged.
- Your delivery address is incomplete.

Do this:

[ ] Do not click the link.
[ ] Do not reply with personal information.
[ ] Do not call the number in the text.
[ ] Do not send verification codes.
[ ] Delete the message if you know it is fake.
[ ] Verify through the official app or website.

Be careful with shortened links

Links from services like bit.ly or tinyurl may hide the real destination.

A shortened link in an unexpected text should be treated carefully.

What Scammers Often Ask For

Be very cautious if anyone asks for:

[ ] Passwords.
[ ] MFA codes.
[ ] Recovery codes.
[ ] Bank account numbers.
[ ] Credit card numbers.
[ ] Social Security numbers.
[ ] Photos of IDs.
[ ] Gift cards.
[ ] Cryptocurrency.
[ ] Wire transfers.
[ ] Zelle, Venmo, Cash App, or PayPal payments.
[ ] Remote access to your computer.
[ ] Login to your bank while they are on the phone.
[ ] Secrecy from family members.

These requests are strong warning signs.

Red Flags by Emotion

Scams often manipulate emotion.

Fear

“You will be arrested.”
“Your account will be closed.”
“Your computer is infected.”
“Your money is at risk.”

Greed or excitement

“You won a prize.”
“You qualify for a refund.”
“You can earn money quickly.”
“This investment is guaranteed.”

Love or sympathy

“I need help.”
“I am in trouble.”
“I cannot tell anyone else.”
“I need money right away.”

Confusion

“This invoice will be charged today.”
“Call to cancel.”
“Your subscription renewed.”
“Your payment failed.”

Trust

“This is your bank.”
“This is Microsoft.”
“This is your boss.”
“This is your grandson.”
“This is the government.”

When a message triggers strong emotion, slow down.

Safer Verification Methods

When you are unsure, use one of these safer methods:

[ ] Open the official app yourself.
[ ] Type the website address directly.
[ ] Call the number on the back of your card.
[ ] Call a family member using a known number.
[ ] Ask a trusted person before sending money.
[ ] Check your real account activity.
[ ] Search for the company’s official website independently.
[ ] Use bookmarks for banking and important accounts.

Do not verify by using the link, phone number, or contact information inside the suspicious message.

What to Do If You Already Clicked

Clicking alone does not always mean damage has occurred.

What matters is what happened next.

If you clicked but did not enter information

[ ] Close the page.
[ ] Do not download anything.
[ ] Do not enter passwords or codes.
[ ] Delete the message.
[ ] Monitor the account if the message claimed to be from a service you use.

If you entered a password

[ ] Change that password immediately from a trusted device.
[ ] Change it anywhere else it was reused.
[ ] Turn on MFA.
[ ] Review account activity.
[ ] Sign out of other sessions if possible.

If you entered a banking password or payment information

[ ] Contact your bank or card issuer immediately.
[ ] Review recent activity.
[ ] Change the password.
[ ] Turn on MFA.
[ ] Consider replacing the card if payment details were exposed.

If you shared an MFA code

[ ] Change the account password immediately.
[ ] Check account activity.
[ ] Sign out of other sessions.
[ ] Review recovery settings.
[ ] Contact the service provider if you suspect takeover.

If you gave remote access

[ ] Disconnect from the internet.
[ ] Shut down the remote access software.
[ ] Change important passwords from a different trusted device.
[ ] Contact your bank if financial information may be involved.
[ ] Consider professional help before using the device normally again.

Special Warning: Verification Codes

A verification code is like a temporary key.

Scammers may say:

- “Read me the code to confirm your identity.”
- “I sent you a code to prove you are real.”
- “Give me the code so I can cancel the charge.”
- “We need the code to secure your account.”

Do not share verification codes.

If someone is asking for the code, they may be trying to log in as you.

Special Warning: Remote Access

Be extremely careful if someone asks to connect to your computer.

Remote access can allow someone to:

- See your screen.
- Move your mouse.
- Open files.
- Install software.
- Access accounts.
- Watch you log in.
- Trick you into sending money.

Do not allow remote access because of an unexpected call, pop-up, email, or text.

Special Warning: Gift Cards and Cryptocurrency

Legitimate companies and government agencies do not ask you to fix urgent problems by paying with gift cards or cryptocurrency.

Be suspicious if someone asks for:

- Apple gift cards
- Google Play cards

- Amazon gift cards
- Steam cards
- Prepaid debit cards
- Bitcoin
- Cryptocurrency transfers
- Wire transfers

These payment methods are often hard to reverse.

Quick Scam Message Checklist

Use this checklist whenever a message feels suspicious.

[ ] Was I expecting this message?
[ ] Does the message create urgency?
[ ] Is it asking me to click a link?
[ ] Is it asking me to call a number?
[ ] Is it asking for money?
[ ] Is it asking for passwords or codes?
[ ] Is the sender address or phone number strange?
[ ] Is the link suspicious?
[ ] Is the grammar, formatting, or tone unusual?
[ ] Is the request unusual for this person or company?
[ ] Can I verify it another way?
[ ] Should I ask someone I trust before acting?

If you checked several boxes, do not proceed until you verify.

Family Safety Script

Use this with relatives, especially older family members.

“If you get a message, call, or pop-up that says something is urgent, do not act right away. Do not click, do not pay, do not share codes, and do not let anyone connect to your computer. Call me first using the number you already know.”

Create a family rule:

No urgent money transfers without direct verification.

Create a family phrase:

If someone claims to be a relative in trouble, they must know the phrase.

Freelancer and Home-Office Reminder

Freelancers and remote workers should be extra careful with:

[ ] Fake clients.
[ ] Unexpected file attachments.
[ ] Fake invoices.
[ ] Fake payment links.
[ ] Overpayment scams.
[ ] Requests to buy equipment.
[ ] Requests to receive and forward money.
[ ] Messages pretending to come from platforms such as LinkedIn, Upwork, Fiverr, PayPal, Stripe, banks, or cloud services.

When money, files, or client data are involved, slow down and verify.

What Not to Do

Do not:

[ ] Click links just because the message looks official.
[ ] Call the phone number in a suspicious message.
[ ] Share passwords.
[ ] Share MFA codes.
[ ] Send money under pressure.
[ ] Give remote access after a pop-up or unexpected call.
[ ] Trust caller ID by itself.
[ ] Trust a message only because it uses your name.
[ ] Ignore your instincts if something feels wrong.
[ ] Feel embarrassed if you are unsure.

Scams are designed to fool people.

Pausing is a strength, not a weakness.

Your Personal Scam Safety Plan

Complete this short plan.

My trusted verification contacts

Trusted person #1: _____

Phone number: _____

Trusted person #2: _____

Phone number: _____

My family verification phrase

Phrase: _____

My most important accounts to protect

[ ] Main email
[ ] Bank
[ ] Credit cards
[ ] Phone carrier
[ ] Apple ID
[ ] Google account
[ ] Microsoft account
[ ] Amazon
[ ] PayPal
[ ] Social media
[ ] Cloud storage
[ ] Password manager

My rule before sending money

I will not send money because of an unexpected message or call until I verify it through a trusted method.

Signature: _____

Date: _____

Final Reminder

Most scam prevention comes down to three habits:

Slow down.
Verify outside the message.
Never share passwords or codes.

If a message makes you panic, pause.

If a message asks for money, verify.

If a message asks for a code, do not share it.

If a message asks for remote access, stop.

Digital safety begins with slowing down long enough to make a better decision.

Click Giraffe Reminder

Click Giraffe is a self-service digital safety membership.

It provides educational guides, checklists, tutorials, monthly scam alerts, and practical resources.

It does not provide live technical support, emergency support, remote access, account recovery, fraud recovery, legal advice, financial advice, medical advice, managed IT services, or guaranteed remediation.

If you are facing fraud, stolen money, identity theft, a compromised account, or an urgent incident, contact the relevant provider, financial institution, law enforcement agency, or qualified professional.