



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples



A Guide to Common Text Message Scams:



Undeliverable Package Scams

The victim receives a text message claiming a package could not be delivered and is asked to pay a fee. Clicking the link opens a fake website that steals payment details.



Employment Scams

The victim receives a text message offering a job they did not apply for. The scammer asks the victim to deposit a check, buy equipment or send money before starting.



Bank Impersonation Scams

The victim receives a text message appearing to be their bank. It warns of suspicious activity and instructs the victim to click a link or call a fake phone number.



Unpaid Road Toll Scams

Victims receive a text message claiming an unpaid road toll is due. The message links to a fake website designed to steal any payment details provided.



IRS Impersonation Scams

Scammers pretend to be the IRS or another tax authority and send messages asking victims to provide personal information or payment details.



Fake Order Notification Scams

Victims are notified an order was placed or a charge was made on their account. The message instructs to call a fake customer support number that is answered by scammers.



Wrong Number Scams

Scammers reach new victims by sending messages to random phone numbers. The scammer attempts to build trust with the victim before attempting an “investment” or “romance” scam.



Outstanding Traffic Ticket Scams

The victim receives a text message claiming there is an outstanding traffic ticket due. The message threatens late fees or legal consequences if payment isn’t made immediately.



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples

Undeliverable Package Scams:

Scammers impersonate delivery services and claim a package was undeliverable. A link to “resolve” opens a fake website that steals any payment details entered. There never was a package.

Undeliverable Package Scam 1:

(Impersonates UPS)

Links to Fake Website

UPS® Ground
Reschedule Your Shipment
Delivery

We attempted to deliver your UPS package on June 23th, but were unable to contact you and the delivery could not be completed. Your package needs to be signed for in person, so please reschedule the delivery by doing the following.

Reschedule Now:

[https://
www.ups.com/package-selector/cc/us](https://www.ups.com/package-selector/cc/us)

Undeliverable Package Scam 2:

(Impersonates USPS)

Malicious File Attached to Message

Text Message
Today 4:16 PM



file_1720728200725.html

HTML text · 16 KB



Dear customer:

Your package has arrived at the distribution facility but we are unable to deliver it due to incomplete address information. Please click on [the html file](#) above to update your address.

The US Postal team wishes you a wonderful day!

Employment Scams:

Scammers impersonate job recruiters offering great pay and benefits, but require the victim to pay upfront for training, supplies, or something else. It's not a real job.

Employment Scam 1:

(Impersonates TikTok Recruitment)

Hello, this is TikTok Recruitment Center. TikTok is one of the most popular short-form video apps with over 2 billion monthly active users, so companies need a rich talent pool. We are now hiring 3,000 TikTok backup talents.

1. People with passion and creativity are needed
2. need responsible employees, and must be adults
3. working hours are 1 hour per day with flexible work location
4. minimum daily salary of \$400, minimum monthly income of \$15,000, paid by the day

If you are passionate and innovative, we invite you to join our team. If you are interested, please contact us on WhatsApp: +19027107508

Employment Scam 2:

(Impersonates Recruiter)

Hello, my name is Lisa and I am a Recruiter at cleanspark. Several recruiting firms have recommended your resume, so our company has an online job for you. This is a free part-time/full-time remote online job with free training. The hours are 30 to 60 minutes per day and the pay is \$200 to \$1,000 per day, not less than \$10,000 per month, paid daily. Regular employees are entitled to 15-30 days of paid annual leave (age 22+ required). If you would like to join us, please contact us on WhatsApp: +13122968793



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples

Unpaid Road Toll Scams:

Scammers impersonate road toll services and claim an unpaid road toll is due. The payment link opens a fake website designed to steal any personal or financial details entered by the victim.

Unpaid Road Toll Scam 1:

(Impersonates Sun Pass)

The Toll Roads Notice of Toll Evasion: You have an unpaid toll bill on your account. To avoid late fees, pay within 12 hours or the late fees will be increased and reported to the DMV.

<https://sunpass.com-etc-lsws.top/vip>

(Please reply Y, then exit the text message and open it again to activate the link, or copy the link to your Safari browser and open it)

The Toll Roads team wishes you a great day!

Unpaid Road Toll Scam 2:

(Impersonates EZPass)

Your recent trip through the New Jersey toll point has incurred an extra \$4.15 charge. To avoid late fees, settle your balance immediately at <https://newjersey-ezpass.com>

Unpaid Road Toll Scam 3:

(Impersonates EzDriveMA)

Your vehicle has an unpaid toll bill. To avoid excessive late fees on your bill, please settle it promptly. Thank you for your cooperation!
Total amount: \$6.99

Payment: <https://ezdrivema.com-paykk.top/i>

Outstanding Traffic Ticket Scams:

Scammers impersonate state agencies and claim an outstanding traffic ticket is due. The link to pay opens a fake website designed to steal any personal or financial details entered by the victim.

Traffic Ticket Scam 1:

Illinois Department of Vehicles(DMV) Final Notice: Enforcement Penalties Begin on July 25.

Our records show that as of today, you still have an outstanding traffic ticket. In accordance with Illinois Code 15C-16.003, If you do not complete payment by July 24, 2025, we will take the following actions:

1. Report to the DMV violation database
 2. Suspend your vehicle registration starting July 25
 3. Suspend driving privileges for 30 days
 4. Transfer to a toll booth and charge a 35% service fee
 5. You may be prosecuted and your credit score will be affected
- Pay Now:

<https://idot.paylmbx.live/pay>

Traffic Ticket Scam 2:

This is a final notice for an unpaid traffic violation. Under New Jersey law (N.J.S.A. Title 39), failure to pay by the deadline will trigger enforcement actions.

Payment Deadline: **January 19, 2026**

If payment is not made by the due date, the following consequences will apply:

1. Report to the New Jersey Motor Vehicle Commission (NJMVC)
2. Vehicle registration automatically suspended on **January 20, 2026**
3. Driver's license suspended for at least 30 days
4. Referral of the outstanding debt to a collections agency, with an additional fee of up to 35%
5. Potential legal proceedings and adverse credit reporting

To avoid these penalties, pay now through the NJMVC official online portal:

<https://nj.govcxe.help/mvc?var=QLqZjEIAgO>



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples

IRS / Tax Department Impersonation Scams:

A message claims you're entitled to a payment or tax refund. It includes a link to confirm your current information. The link opens a fake website designed to steal any personal and financial details entered.

IRS Impersonation Scam:

Internal Revenue Service (IRS)

You are eligible to receive a \$1,400 Economic Impact Payment. Please provide your accurate personal information. We will deposit the amount into your bank account or mail a paper check within 1 to 2 business days.

<https://www.irs.gov.subsidy-ion.com>

(Please reply with "Y," then exit the text message. Open it again, click the link, or copy it into your Safari browser and open it.)

Department of Taxation Impersonation Scam:

New Jersey Department of Taxation

Your refund request has been processed and approved. Please provide accurate payment information by September 16, 2025. Funds will be deposited into your bank account or mailed to you via paper check within 1-2 business days.

<https://nj.com-casgu.my/state>

Wrong Number Scams:

Scammers reach new victims by sending messages to random phone numbers. When someone replies, the scammer gains the victim's trust then attempts an "investment" or "romance" scam.

Wrong Number Scam (Text Message):

Hi

*hi who's this

I'm Karina. Are you David? And we met last week at Linda's party, and you picked this number for me

Hi sorry you have the wrong number

Oh my gosh. I checked and found out I entered the wrong area code. I hope this doesn't bother you

Thats ok no problem

Thank you very much. You are a very friendly and polite person, I hope we can be friends. Nice to meet you, my name is Karina, what can I call you?

you have a beautiful name, i am from malaysia and currently living in los angeles. where do you live

Pat



Common Text Message Scams

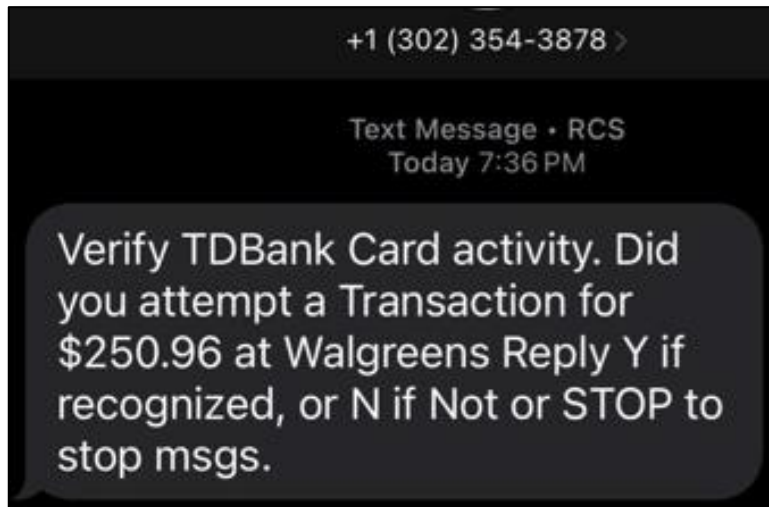
A Guide to Common Text Message Scams + Real Scam Examples

Bank Impersonation Scams:

Scammers impersonate the bank claiming suspicious activity was detected. Victims are instructed to “secure” their money by unknowingly sending it to scammers.

Bank Impersonation Scam (Text Message):

- Text message impersonates TDBank (it's a scammer)
- Claims debit card was used at Walgreens
- Instructs victim to reply, then will initiate a phone call



Warning: This type of scam often starts with a phone call, text message or email from a scammer. Be suspicious of anyone claiming to be “the bank.”



Automated
phone calls



Text
messages

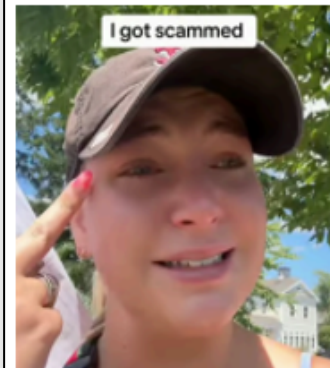


Emails

Bank Impersonation Scam (Phone Call): Victim's Story

- Incoming phone call from a trusted Wells Fargo number shown on caller id
- Claims fraudulent activity was detected and funds must be secured
- Victim is instructed to transfer money using Zelle to secure the funds

'I feel so stupid': This young Connecticut woman had her bank account drained by scammers after answering trusted Wells Fargo number — how to spot and avoid similar schemes



Stenz's trouble began when she saw a familiar phone number on her caller ID.

*"I got a **call from a Wells Fargo number** saying I had fraudulent activity on my account and that a random person was being sent money from Zelle."*

"They told me to secure my account by sending money that would go back to my account right after."

Source:

<https://www.the-sun.com/money/12745806/wells-fargo-customers-account-drained-zelle-transaction-scam/>



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples

Fake Order Notification Scams:

Victims are notified that an order was placed and instructed to call a phone number to dispute it. Dialing the number calls a scammer who then impersonates customer support.

Fake Order Notification Scam (Text Message):

Apple Approval Notice

We have noticed that your Apple iCloud id was recently used at "APPLE STORE - CA" for \$143.95, paid by Apple Pay Pre Authorization. Also some suspicious sign in request and apple pay activation request detected. That looks like suspicious to us. In order to maintain the security and privacy of your account we have placed those request on hold. If NOT you? talk to an Apple Representative. Failing may lead to auto debit and charge will not be reversed. Call [+1 8773055161](tel:+18773055161) immediately to cancel this charge.

Billing Department : <https://>

- Text message impersonates Apple
- Claims a purchase was made
- Includes a phone number to dispute
- Dialing the number calls a scammer

Warning: This type of scam often starts with a phone call, text message or email from a scammer. Stay alert and suspicious of order notifications.



Automated
phone calls



Text
messages



Emails

Fake Order Notification Scam (Email): Victim's Story

- Email impersonates Apple, claims an iPhone was purchased
- Includes a fake phone number to dispute the charge
- Calling the number connects to a scammer



News Weather Sports Pure Nebraska Contact Us



By [Abigail Carrera](#)

Published: Aug. 2, 2024 at 12:08 PM EDT | Updated: Aug. 2, 2024 at 12:34 PM EDT



LINCOLN, Neb. (KOLN) - A 23-year-old Lincoln woman reported losing \$4,100 after falling victim to an identity fraud scam in July, Lincoln Police said.

The scam began on July 17 with an email claiming she had purchased an iPhone. The woman called the number provided in the email to dispute the purchase and was told she had multiple open accounts in her name across various states. She was informed someone was using her identity.

According to police, scammers then connected the woman to a person posing as a "CIA agent" who instructed her to withdraw \$3,600 from her bank account. The next day, she was directed to use the money to purchase Walmart cash cards and send photos and receipts. Additionally, the woman sent another \$500 cash card to the scammers.



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples



Stay Safe from Text Message Scams:



Assume **every unsolicited communication** is a scammer.



Access Websites Directly (Instead of Clicking Links)

Scam text messages often include links that lead to fake websites designed to steal your information. Instead of clicking the link, type the website address directly into your internet browser to make sure you are visiting the real, trusted site.



Verify Phone Numbers Before Calling Back

Scammers often include fake phone numbers in text messages to trick you into calling them. Before calling back, take a moment to look up the organization's real phone number and make sure it matches.



Confirm Situations Through Official Channels

If a text message says an order was placed or your account is locked, do not reply or click on anything. Instead, check your account directly using the official website or app. Only call phone numbers listed on the organization's official website – make sure it's their real website and real phone number.



Dangerous Actions to Avoid:



Knowing **what NOT to do**, is how you **avoid traps** set by scammers.



Replying to Text Messages from Unknown Senders

Replying lets scammers know your phone number is active, which can lead to more scam messages. It's best to ignore the text. Block and delete it.



Clicking Links or Opening Attachments in Text Messages

Links and attachments can take you to fake websites that steal personal or financial information. Do not click links, open attachments, or scan QR codes from unexpected texts.



Trusting the Name or Number Shown on Caller ID

Scammers can fake the name or number that appears on your phone. Messages may look like they come from a bank, delivery company, or government agency when they do not.



Calling Back Phone Numbers from Unsolicited Texts

Scam texts often include phone numbers that connect directly to scammers. Always look up the organization's real phone number on their official website before calling.



Common Text Message Scams

A Guide to Common Text Message Scams + Real Scam Examples

Stay Scam Aware! More From ScamAware101

Everyone should have the knowledge to defend against scams!

ScamAware101: Online Courses, Webinars, Group Presentations, Scam Alerts

SCAM AWARENESS LIVE: EVERY THURSDAY (WATCH ON YOUTUBE)



SCAM AWARENESS LIVE STREAM

Everyone should have the knowledge to defend against scams...

Scam Awareness Live: Every Thursday on YouTube!

-  20+ Common Scams Targeting Individuals (YOU)
-  Red Flags to Identify and Prevent a Scam
-  Real Examples of Recent Scams:
 - Email Scams (Phishing Emails)
 - Phone Call Scams (Recordings)
 - Text Message Scams (Screenshots)
 - Snail Mail Scams (Letters/Postcards)



Watch Live Stream on YouTube:
[youtube.com/@scamaware101](https://www.youtube.com/@scamaware101)



Presented By: Jared Caldara
Founder of ScamAware101
<https://www.scamaware101.com>

Follow ScamAware101:

<https://www.ScamAware101.com>

<https://www.youtube.com/@scamaware101>

<https://www.facebook.com/scamaware101>



ScamAware101 Mailing List

Stay Informed and Prepared for Scams

- Scam Alerts and Warnings
- Live Stream Reminders
- News & Announcements
- New Content Notifications



JOIN THE MAILING LIST BY VISITING:
[ScamAware101.com](https://www.ScamAware101.com)



Scam Awareness Courses

Online Courses for Everyday People

- No Prior Knowledge Needed
- Learn at Your Own Pace
- Easy and User Friendly
- Learn from Real Experts
- Practical Real-Life Examples



VIEW ONLINE COURSES BY VISITING:
[ScamAware101.com](https://www.ScamAware101.com)