

The 12 Most Common Text Scams

How to spot and
how to avoid



Fake Package Delivery Scam



Risk Level:
Critical



Description: A text claims there's a problem with a package delivery.



How the Scam Is Perpetrated:
Scammers impersonate USPS, UPS, FedEx, or Amazon and send a link.



Who Is Usually Involved:
Fraudsters posing as shipping carriers.



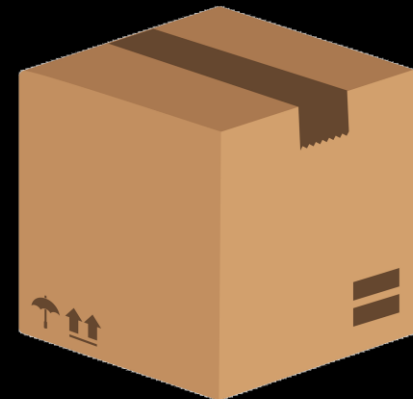
End Goal: Steal credit card numbers or personal info.



Warning Signs:
Unexpected delivery notices and misspelled URLs.



How to Protect Yourself: Never click links; go directly to the carrier's official website.



Smishing (General Phishing)



Risk Level: **High**



Description:
Someone
pretends to be a
friend or family
member in
trouble.



How the Scam Is
Perpetrated:
**Scammers
request login
credentials or
financial info.**



Who Is Usually
Involved:
**Cybercriminals
impersonating
banks or utilities.**



End Goal:
Identity theft.



Warning Signs:
**Urgent language
and requests for
personal info.**



How to Protect
Yourself: **Never
click links;
Ignore the text;
contact the
company
directly.**



Imposter / Family Emergency Scam



Risk Level:
Critical



Description: A text pretending to be from a legitimate company.



How the Scam Is Perpetrated:
Scammers claim emergencies and request money.



Who Is Usually Involved:
Fraudsters using social media info.



End Goal:
Immediate financial theft.



Warning Signs:
Requests for gift cards and secrecy.



How to Protect Yourself: **Call the real person directly.**



Fake Fraud Alert (Bank/Amazon)



Risk Level: **High**



Description: A text claims suspicious activity on your account.



How the Scam Is Perpetrated: Scammers direct you to call a fake fraud department.



Who Is Usually Involved: Scammers posing as banks or Amazon.



End Goal: Trick you into transferring money.



Warning Signs: Account lockout claims and urgent instructions.



How to Protect Yourself: Call your bank using the number on your card.



Bogus Toll Road Fees



Risk Level:
Medium



Description: A text claims you owe an unpaid toll.



How the Scam Is Perpetrated:
Scammers impersonate toll systems.



Who Is Usually Involved: **Fraud rings targeting drivers.**



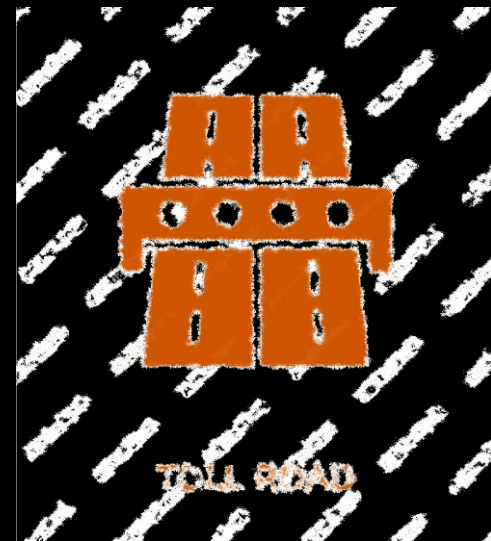
End Goal: **Steal credit card info.**



Warning Signs:
Final notice language and unfamiliar domains.



How to Protect Yourself: **Check your toll account directly.**



Malware Link Scam



Risk Level:
Medium



Description: A
text contains a
harmful link.



How the Scam Is
Perpetrated:
**Scammers install
malware or
spyware.**



Who Is Usually
Involved:
Cybercriminals.



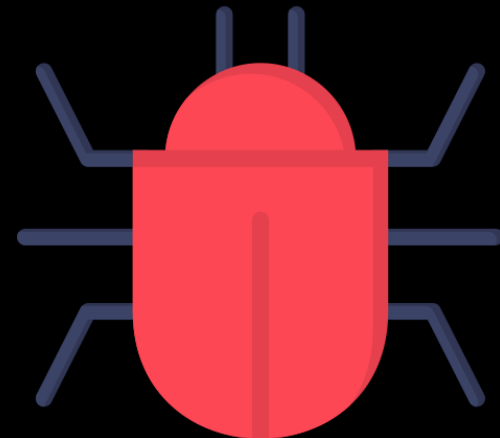
End Goal: **Gain
access to your
device or
accounts.**



Warning Signs:
**Random links
and unknown
senders.**



How to Protect
Yourself: **Never
click unknown
links.**



Fake Lottery / Prize Scam



Risk Level:
Medium



Description: A text claims you won a prize.



How the Scam Is Perpetrated:
Scammers ask for fees or bank info.



Who Is Usually Involved:
Fraudsters posing as contest organizers.



End Goal: **Steal money or personal info.**



Warning Signs:
You never entered the contest.



How to Protect Yourself: **Ignore; real contests never charge winners.**



Job / Task Scam



Risk Level:
Medium



Description: A text offering easy money.



How the Scam Is Perpetrated:
Scammers demand payment to unlock earnings.



Who Is Usually Involved: Fake recruiters.



End Goal:
Financial Theft.



Warning Signs:
No interview and upfront fees.



How to Protect Yourself: Avoid jobs requiring payment.



Bank Account Verification Scam



Risk Level: **High**



Description: A text asks you to verify bank details.



How the Scam Is Perpetrated: **Scammers impersonate banks.**



Who Is Usually Involved: **Fraudsters using spoofed numbers.**



End Goal: **Steal login credentials.**



Warning Signs: **Requests for PINs or passwords.**



How to Protect Yourself: **Banks never ask for sensitive info by text.**



Subscription Renewal Scam



Risk Level:
Medium



Description: A text claims your subscription is renewing.



How the Scam Is Perpetrated:
Scammers pressure you to call a number.



Who Is Usually Involved:
Call-center fraud groups.



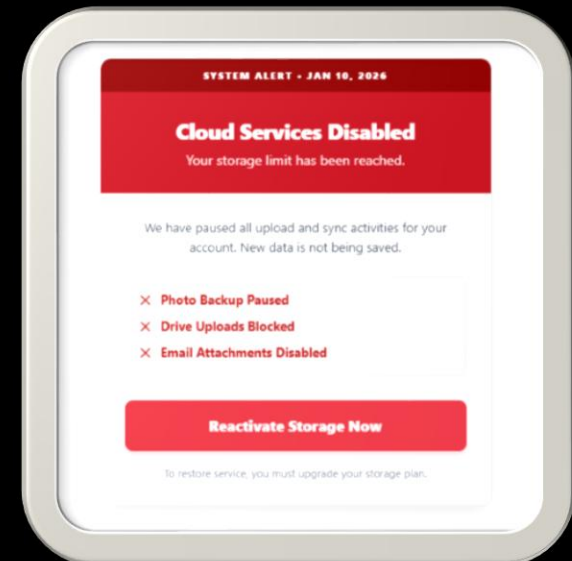
End Goal:
Remote access or payment theft.



Warning Signs:
Threats of large charges.



How to Protect Yourself: **Check your real subscriptions.**



Fake Charity / Disaster Relief Scam



Risk Level: **Low**



Description: A text asks for donations.



How the Scam Is Perpetrated: **Scammers exploit emotional events.**



Who Is Usually Involved: **Fraudster posing as nonprofits.**



End Goal: **Steal money.**



Warning Signs: **Requests for gift cards and no official website.**



How to Protect Yourself: **Donate only through verified charity sites.**



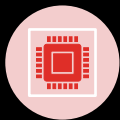
Account Suspension Scam (IRS/SSA/DMV)



Risk Level: **High**



Description: A text claims your government account is suspended.



How the Scam Is Perpetrated: **Scammers impersonate agencies.**



Who Is Usually Involved: **Fraud rings using spoofed caller IDs.**



End Goal: **Identity theft.**



Warning Signs: **Government agencies do not text.**



How to Protect Yourself: **Ignore and report.**

