New Amazon "Product Recall" Message Scam: What It *Really* Is and What You Should Do

Security researchers are warning about a new phishing attack targeting Amazon users right now. It looks like this:

You get a text message saying there's a product recall on something you bought from Amazon. The message includes a link to "view details" or "resolve the recall."
But here's the catch: the link doesn't go to Amazon; it goes to a realistic-looking fake Amazon login page. If you enter your credentials there, attackers steal your username and password.

This is classic phishing designed to hijack your Amazon account. That means the scammers want access to your account so they can do things like:

- Steal saved payment info
- Make unauthorized purchases
- Change your orders
- See personal details
-

Why This Works

Attackers are using a trigger that feels urgent and legit, a product recall alert, to get you to click the link without thinking. It's the same basic tactic we've seen in email scams, but it is also being used in text messages too. The tricks are always the same, create a sense of urgency, fear, or panic, that you need to do something now. This tactic is called Social Engineering. You can read about this in an upcoming part of our AI and Its Impact on Cybersecurity series. Go to our Resource page at KnowPhishing.com.

What Should You Do, or NOT Do

1. **Never click links in unexpected texts.**
   If a message says there's a recall or problem, go into your actual Amazon app or website, do not tap anything in the message.
2. **Check the sender details.**
   Scams often come from random phone numbers or spoofed addresses that don't match official Amazon messaging.
3. **Don't enter your login info on a page you reached from a link in a message.**
   If you're unsure, close the browser and go to amazon.com yourself.

4. **Watch for urgency and pressure language.**
   "Your account will be closed!" or "Act now!" are classic phishing hooks.
5. **Report the message as spam/phishing.**
   On iPhone or Android you can mark the text as junk and report it.
6. **Turn on MFA (Multi-Factor Authentication).**
   That adds an extra layer of protection even if your password gets compromised.

Bottom Line

If you get a text about an "Amazon product recall" with a link, treat it as malicious until proven otherwise. This is a phishing tactic, not a legitimate Amazon notification, and the goal is to steal your credentials, plain and simple.
Stay cautious and always double-check messages like this, your logins and money depend on it.