14 scam messages to watch out for in 2023

By Jim Martin, Executive Editor, Tech Advisor JUL 21, 2023

The most popular phrases scammers use to trick you into giving them your details

Phishing scams are everywhere now, and they're easy to fall for. According to recent research by Norton, two thirds of cyberattacks so far this year have been phishing scams. No doubt you've seen some in your email inbox already, or maybe in text messages sent to your phone.

They usually work on the basis of fear: a message worrying enough to make you click the link to fix whatever the problem is.

Whether that's a problem with your payment details which will cause a service or subscription to stop or a missed delivery that needs to be rearranged, scammers will send messages that appear to come from genuine companies.

If you do click on the link that's inevitably included somewhere in the message, you'll likely arrive at a fake version of the company's website with a login screen or a form to fill out details such as your name and address, maybe even payment information.

And if you don't realise it's a fake and type it in anyway, you'll send those personal details straight to the scammers who will use them to log into your real account (and maybe others if you reuse the same email and password combination) or steal your identity and use it to take out loans and other fraudulent activity.

As well as watching out for the common subject lines below, you should also train yourself to refrain from tapping or clicking on a link until you've made sure it isn't a scam.

These are just examples, and the messages in your inbox or on your phone might use a different company name or be phrased slightly differently.

1. Your Netflix membership has ended, because we're having some trouble with your current account information.
2. Your Apple Pay has been suspended, please update your details by visiting: <link>
3. Verify your account within 24 hours or your PayPal account will be terminated permanently. Regards, PayPal
4. Reminder: If overdue records are not processed, it will affect your credit.
5. Your package cannot be delivered due to an incorrect house number.
6. Your online account is temporarily locked due to an unusual sign in attempt. Please login and confirm your information. <link>
7. DANGER: A THREAT has INFECTED your LAPTOP! ACT NOW to PROTECT your CONFIDENTIAL FILES at <link>
8. You Can Get PAID $100 for taking this 2-minute Survey!
9. Your payment is overdue. Please avoid your fine charge please see <link>
10. Hi Your FEDEX parcel with tracking <|number|> is waiting for you to set delivery preferences: <link>
11. Amazon: your account has been locked due to suspicious activity: <link>. Click the link below to unlock your account.
12. [Inland Revenue] You have a pending refund. Please collect it now at: <link>
13. myGov: Your income return of [amount] could not be processed due to insufficient information supplied please update immediately at <link>
14. eFlow: You have been recorded using the motorway without paying the appropriate charge(s) of 6.40 visit <|url|> or an additional fine of 97.50 will be sent to your home address.

Not all phishing scams rely on fear. Some, such as getting paid for filling out surveys, work on that basis that you'll hand over personally identifiable information in return for a reward. In some cases these might be genuine, but even after verifying that it isn't a scam, consider whether the reward is really worth handing over that information.

It's also a good idea to run security software on your devices – both your laptop and phone – that can flag fake websites and even potentially dangerous links in messages like these. Then you won't have to rely on spotting these scams yourself.