A word about email and internet scams:

Scammers use email or text messages to trick you into giving them your personal and financial information. But there are several ways to protect yourself.

What is phishing (pronounced just like 'fishing')?
Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money.

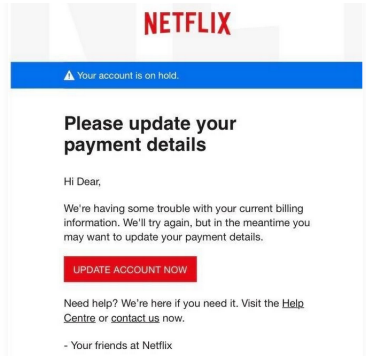
How does a phishing attack work?Phishing attacks begin with the threat actor sending a communication, acting as someone trusted or familiar. The sender asks the recipient to take an action, often implying an urgent need to do so. Victims who fall for the scam may give away sensitive information that could cost them. Here are more details on how phishing attacks work:

The sender: In a phishing attack, the sender imitates (or "spoofs") someone trustworthy that the recipient would likely know. Depending on the type of phishing attack, it could be an individual, like a family member of the recipient, the CEO of the company they work for, or even someone famous who is supposedly giving something away. Often phishing messages mimic emails from large companies like PayPal, Amazon, or Microsoft, and also banks or government offices.

The message: Under the guise of someone trusted, the attacker will ask the recipient to click a link, download an attachment, or to send money. When the victim opens the message, they find a scary message meant to overcome their better judgment by filling them with fear. The message may demand that the victim go to a website and take immediate action or risk some sort of consequence.

The destination: If users take the bait and click the link, they're sent to an imitation of a legitimate website. From here, they're asked to log in with their username and password credentials. If they are gullible enough to comply, the sign-on information goes to the attacker, who uses it to steal identities, pilfer bank accounts, and sell personal information on the black market.

Here's a real-world example of a phishing email:



Imagine you saw this in your inbox. At first glance, this email looks real, but it's not.

Scammers who send emails like this one are hoping you won't notice it's a fake.

Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company's logo in the header:

The email has a generic greeting. The opening to this email "Hi Dear" is a red flag that this is a scam. Don't click any links and log into your account via Netflix.com directly.

The email says your account is on hold because of a billing problem.

The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

DO NOT EVER CLICK ON AN EMAIL LINK! If you have any doubts as to any online account, log in as you normally would and check on it; but never by clicking on an email link.