THE FTC IS CLOSED DUE TO THE LAPSE IN FUNDING. :

Learn about the status of FTC online services and website information updates during the lapse in funding.

FEDERAL TRADE COMMISSION

Consumer Information

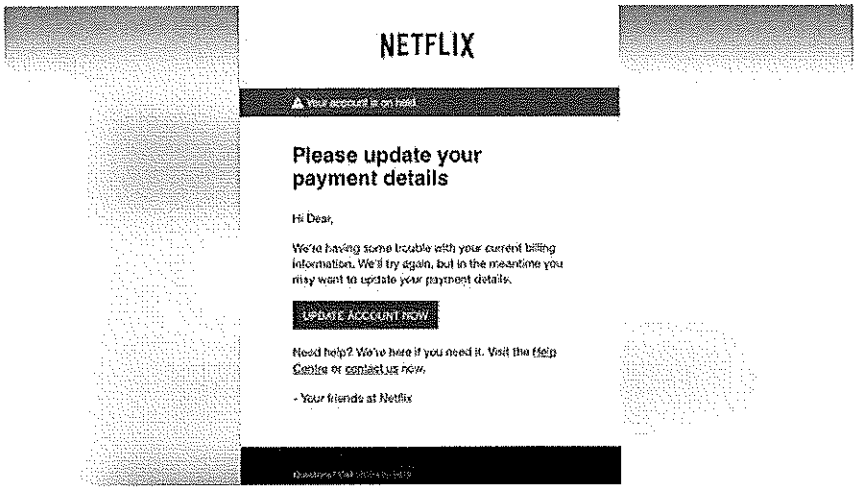
consumer.ftc.gov

Netflix phishing scam: Don't take the bait

December 26, 2018
by Colleen Tressler
Consumer Education Specialist, FTC

Phishing is when someone uses fake emails or texts to get you to share valuable personal information – like account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money, your identity (https://www.consumer.ftc.gov/articles/0005-identity-theft), or both. They also use phishing emails to get access to your computer or network. If you click on a link, they can install ransomware (https://www.consumer.ftc.gov/blog/2016/11/how-defend-against-ransomware) or other programs that can lock you out of your data.

Scammers often use familiar company names or pretend to be someone you know. Here's a real world example featuring Netflix. Police in Ohio shared a screenshot of a phishing email designed to steal personal information. The email claims the user's account is on hold because Netflix is "having some trouble with your current billing information" and invites the user to click on a link to update their payment method.



Before you click on a link or share any of your sensitive information:

- **Check it out.** If you have concerns about the email, contact the company directly. But look up their phone number or website yourself. That way, you'll know you're getting the real company and not about to call a scammer or follow a link that will download malware (https://www.consumer.ftc.gov/articles/0011-malware).
- **Take a closer look.** While some phishing emails look completely legit, bad grammar and spelling can tip you off to phishing. Other clues: Your name is missing, or you don't even have an account with the company. In the Netflix example, the scammer used the British spelling of "Center" (Centre) and used the greeting, "Hi Dear." Listing only an international phone number for a U.S.-based company is also suspicious.
- **Report phishing emails.** Forward them to *spam@uce.gov (mailto:spam@uce.gov)* (an address used by the FTC) and to *reportphishing@apwg.org (mailto:reportphishing@apwg.org)* (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). You can also report phishing to the FTC at *ftc.gov/complaint (https://www.ftccomplaintassistant.gov/)*. Also, let the company or person that was impersonated know about the phishing scheme. For Netflix, forward the message to *phishing@netflix.com (mailto:phishing@netflix.com)*.

For more tips and information, visit this article on phishing (https://www.consumer.ftc.gov/articles/0003-phishing). Then test your knowledge by playing this game (https://www.consumer.ftc.gov/media/game-0011-phishing-scams).

Blog Topics: Money & Credit (https://www.consumer.ftc.gov/blog/money-%26-credit)