BUSINESS IMPOSTOR SCAMS: STREAMING SERVICES AND INTERNET PROVIDERS

Business impostor scams often target consumers by impersonating streaming services or internet service providers. These scams typically begin with an alarming text message, email or phone call warning of a service disruption or promoting a limited-time, too-good-to-be-true offer. Fraudulent offers also may appear as ads or links on social media platforms.
The goal: trick you into providing personal information to criminals, such as passwords, credit card numbers and bank account details.

Business Impostor Scam*: A type of deception where an individual poses as a legitimate business, company or brand to deceive a victim into making payments or providing sensitive information.

Criminals create a sense of urgency, warning that service may be interrupted without an immediate payment or that a special deal expires soon. Messages often include callback numbers or links to fake websites that appear to be legitimate. These sites are convincing because they use authentic-looking logos and layouts to deceive victims and capture login credentials and financial information.

HOW TO PROTECT YOUR ACCOUNTS AND INFORMATION

1. Don't trust pop-up or unsolicited messages or phone calls
2. Be suspicious of pressure tactics and unusual payment requests
3. Look for spoofed texts, emails and websites – which are manipulated to appear to be from a trusted source or legitimate organization but are slightly different than the real business' texts, emails or website addresses
4. Don't click on suspicious links or attachments in phishing (impersonated) messages that can lead to fraudulent websites or install malware on your device
5. Verify account status or special offers directly with providers, and do so by using only their official websites, apps or support phone numbers
6. Report scams promptly to the legitimate organization being impersonated, contact local law enforcement and alert your financial institution(s) if you've made any payments

BUSINESS IMPOSTOR SCAMS: STREAMING SERVICES AND INTERNET PROVIDERS

EXAMPLES OF PHISHING EMAILS

Phishing Email: Monthly Subscription Renewal

Victims receive a message claiming their monthly payments or subscription renewals could not be processed, urging immediate action to prevent service disruptions or account closures. These messages direct recipients to "resolve the issue" by updating login credentials and payment information on a fraudulent website. Conversely, these websites are designed to enable criminals to capture sensitive data, including account access details and payment information.

Email Message: Unable to process monthly subscription payment

Sender: *MySubscription*

Subject: *We were unable to process your subscription payment for this month.*

Hello:
Your renewal couldn't be completed.

A quick update to your payment method is required to keep your access active. We tried processing your subscription renewal, but the payment was declined. This can happen for several reasons — such as an expired card, outdated billing info or your bank blocking the charge.

To avoid any interruption, please review and update your payment method. Your service will automatically resume when the payment is processed.

Sincerely,
Customer Service team

BUSINESS IMPOSTOR SCAMS: STREAMING SERVICES AND INTERNET PROVIDERS

Phishing Email: Account Suspended

Phishing emails or text messages may claim that a customer's account has been suspended due to suspicious activity or a violation of the terms of service. These messages often include an alert stating that someone has reported the account to an administrator and that a response is required within 24 hours to avoid permanent closure.

Email message: Your account is suspended

Sender: *Email Administrator*

Subject: *Your account is suspended*

Dear Customer:

Your account has been suspended due to suspicious activity. Your immediate attention is needed to restore your service. Verification must be completed within 24 hours to avoid account termination. Click here to enter the required information and complete validation.

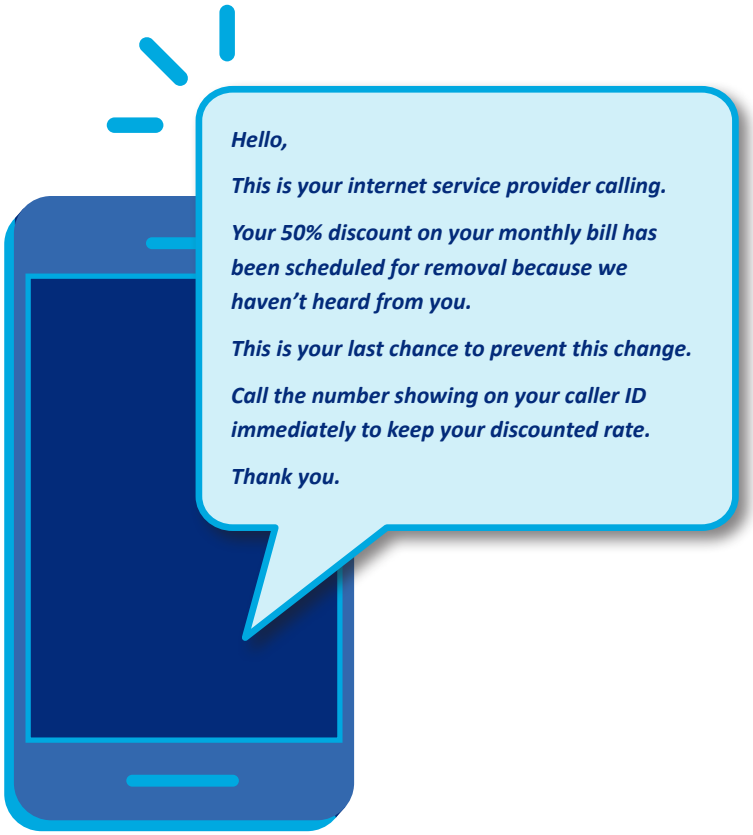
Account Services

BUSINESS IMPOSTOR SCAMS: STREAMING SERVICES AND INTERNET PROVIDERS

Phishing Phone Message: Limited-Time Offer or Expiring Discount

Criminals send messages promoting a new offer available for a limited time or warning the recipient that an existing discount is about to expire. These messages are designed to create urgency and prompt immediate action. Victims typically are instructed to respond using a link or phone number, offering a substantial discount (50% or more) to increase engagement.

In some cases, no callback number is provided. Instead, recipients are told to use the phone number displayed on their caller ID. These tactics aim to direct victims to fraudulent websites or contact centers, where personal and payment information can be harvested.



CONCLUSION

It is easy to be tricked by a business impostor scam when the email looks legitimate and pressures you to respond. Always be cautious of emails from companies that are alerting you to avoid an imminent service cancellation requiring immediate action and/or payment information. It is best to contact the company directly through its website, app or phone number to confirm information in the email.

* Business impostor scam definition taken from ScamClassifer Model and Definitions.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, use of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.