Email Analysis Report

From: Account Support <support@marine-patrimoine.fr>
Sent: Sunday, September 27, 2020 10:08:05 PM
To: bhavinparmars@outlook.com <bhavinparmars@outlook.com>
Subject: Re :[Reminder September Information] Your account was used to sign in at Microsoft Edge from Iran (Islamic Republic of) - Nuovo estratto conto e account aggiornati inviati per reimpostare la password di accesso [Codice servizio-97854.]

Your Account Has Been Limited!

Case id : 9000321-58336 `Login attempt from unkown device.`

Dear Client,

It looks like someone else may have acces to your account, so we've temporarily locked it to keep your personal informations in safe. To unlock your account, you may need to pass a security check. Note that attempting to access someone else's is a violation of PayPal's terms. It may also be illegal.

To reset your account access please enter the link below :

Secure Your Account

(https://duapuluhtujuhgasterus.coincidenceinhide.com/r/jIPk5WJ)

Yours sincerely,

PayPal

Red Flags Identified

- **Suspicious sender domain: Email is from 'marine-patrimoine.fr' instead of PayPal.com**
- **Urgency: Threatens account limitation to scare the user**
- **Suspicious login location: Claims login from Iran, creating panic**
- **Strange subject line: Includes mixed language and irrelevant details**
- **No real PayPal branding or formatting: Plain text and no professional look**
- **Generic greeting: Uses 'Dear Client' instead of your real name**
- **Suspicious link: Encourages clicking on a fake 'Secure Your Account' link**

How to Avoid Falling for It

- **Always check the sender’s email address carefully**
- **Never click on suspicious or shortened links in emails**
- **Look for your real name – legit companies don’t say 'Dear Client'**
- **Ignore emails that pressure you to act immediately**
- **Report phishing emails to your provider or company (like spoof@paypal.com)**

Summary

This phishing email was designed to look like a PayPal alert but came from a suspicious domain. It used panic tactics such as foreign logins and account lock warnings. Several red flags such as generic language, fake links, and urgency were identified. The report shows how awareness and basic checks can help prevent falling for phishing scams.