UNIVERSITY OF MARYLAND EXTENSION | Marylanders Online

## STAY SAFE ONLINE:

# AVOIDING SCAMS MADE EASY!

### 1 Suspicious Messages? Pause and Think!

If you weren't expecting a message, be careful. Check who sent it — strange names or numbers can be scams. Watch for bad grammar or urgent warnings. Hover over links without clicking; **if they look odd, don't trust them.**

### 2 Avoid Scam Websites and pop-ups

**Be careful when browsing online. Some websites and pop-ups are designed to trick you.** They might offer free prizes, fake virus warnings, or urgent messages. If a site looks strange, has lots of pop-ups, or asks for personal information right away, close it and leave.

### 3 Protect Your Personal Information


Think before you share personal details online. Only enter your name, address, passwords, or bank information on trusted websites. **If a website, message, or app asks for too much information, it's a good idea to stop and check if it's safe first.**

### 4 Not Sure What to Do?

If something feels wrong, trust your instincts and stop right away. **Do not click, reply, or give any information**. Take a screenshot of the message or site if you can. Then, check with a trusted person, search for the company's official website yourself, or report the scam to your email provider or a help center. It's always better to be safe than sorry.

English and Spanish tech support available.

1-866-206-8467, Monday-Friday, 10 a.m. - 8 p.m., Saturday, 10 a.m. - 5 p.m.
marylandersonline@umd.edu

Get Connected with
**Marylanders Online**

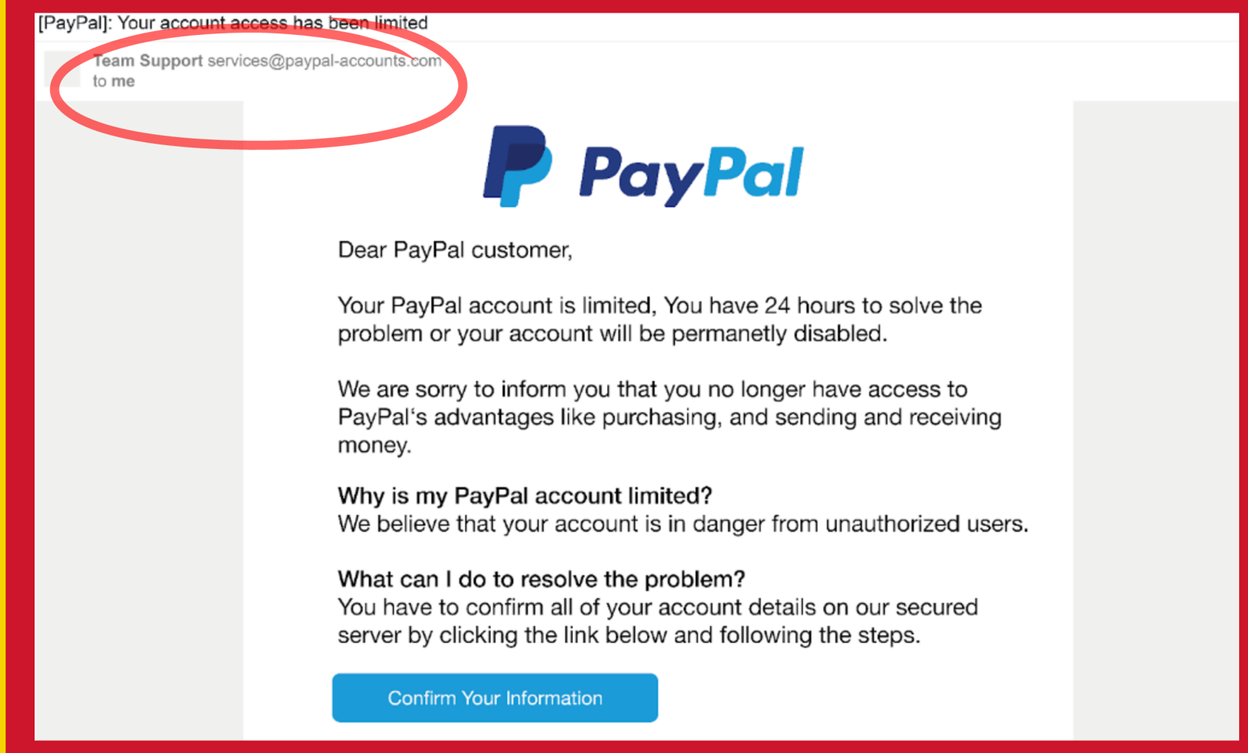
Contact us today for **FREE** one-on-one tech support and internet training.

UNIVERSITY OF MARYLAND EXTENSION | Marylanders Online

## STAY SAFE ONLINE:

# SPOTTING SCAMS FAST

## Phishing Alert!


[PayPal]: Your account access has been limited

**Team Support** services@paypal-accounts.com
to me

PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

**Why is my PayPal account limited?**
We believe that your account is in danger from unauthorized users.

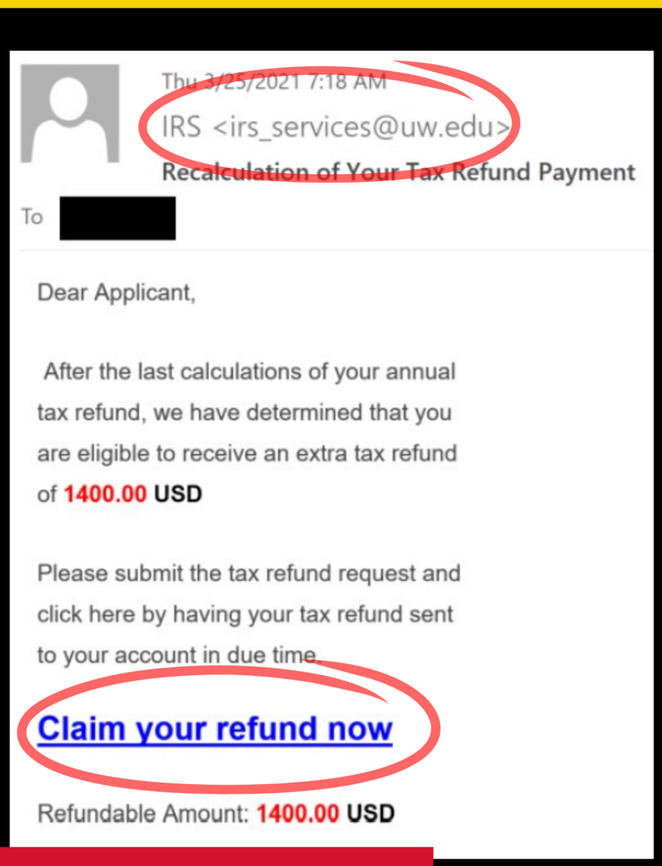
**What can I do to resolve the problem?**
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

**Phishing** is when scammers pretend to be a trusted company or person to trick you into giving away sensitive information, like passwords, credit card numbers, or bank details.

For example, this message is a scam because the email address is not from PayPal's official support, which is service@paypal.com.

**English and Spanish tech support available.** | **1-866-206-8467, Monday-Friday, 10 a.m. - 8 p.m., Saturday, 10 a.m. - 5 p.m. marylandersonline@umd.edu**


Thu 3/25/2021 7:18 AM
IRS <irs_services@uw.edu>
Recalculation of Your Tax Refund Payment
To [redacted]

Dear Applicant,

After the last calculations of your annual tax refund, we have determined that you are eligible to receive an extra tax refund of 1400.00 USD

Please submit the tax refund request and click here by having your tax refund sent to your account in due time.

Claim your refund now

Refundable Amount: 1400.00 USD

We can tell this is a scam because the message pretends to be from the IRS, but the email address is fake. Real government emails don't come from school domains, and they never ask you to click links to claim a refund.

## 4 Common Scam Red Flags:

1. **Strange sender address:** Not from an official website or company.
2. **Urgent or scary language:** Rushing you to act fast.
3. **Suspicious links:** Asking you to click without explaining why.
4. **Requests for personal information:** Asking for passwords, money, or personal details.