Employee Cybersecurity Awareness Training

Mike Tech Show

September 2025

Why Cybersecurity Matters

- 90% of data breaches start with phishing emails
- Risks: data theft, financial loss, reputation damage
- Every employee is the first line of defense

Common Cyber Email Threats

- Phishing & spear phishing – *fake messages that look real*.
- Business Email Compromise – *attackers impersonate executives*.
- Malware & ransomware– *malicious attachments or links*.
- Credential harvesting - *fake login pages*

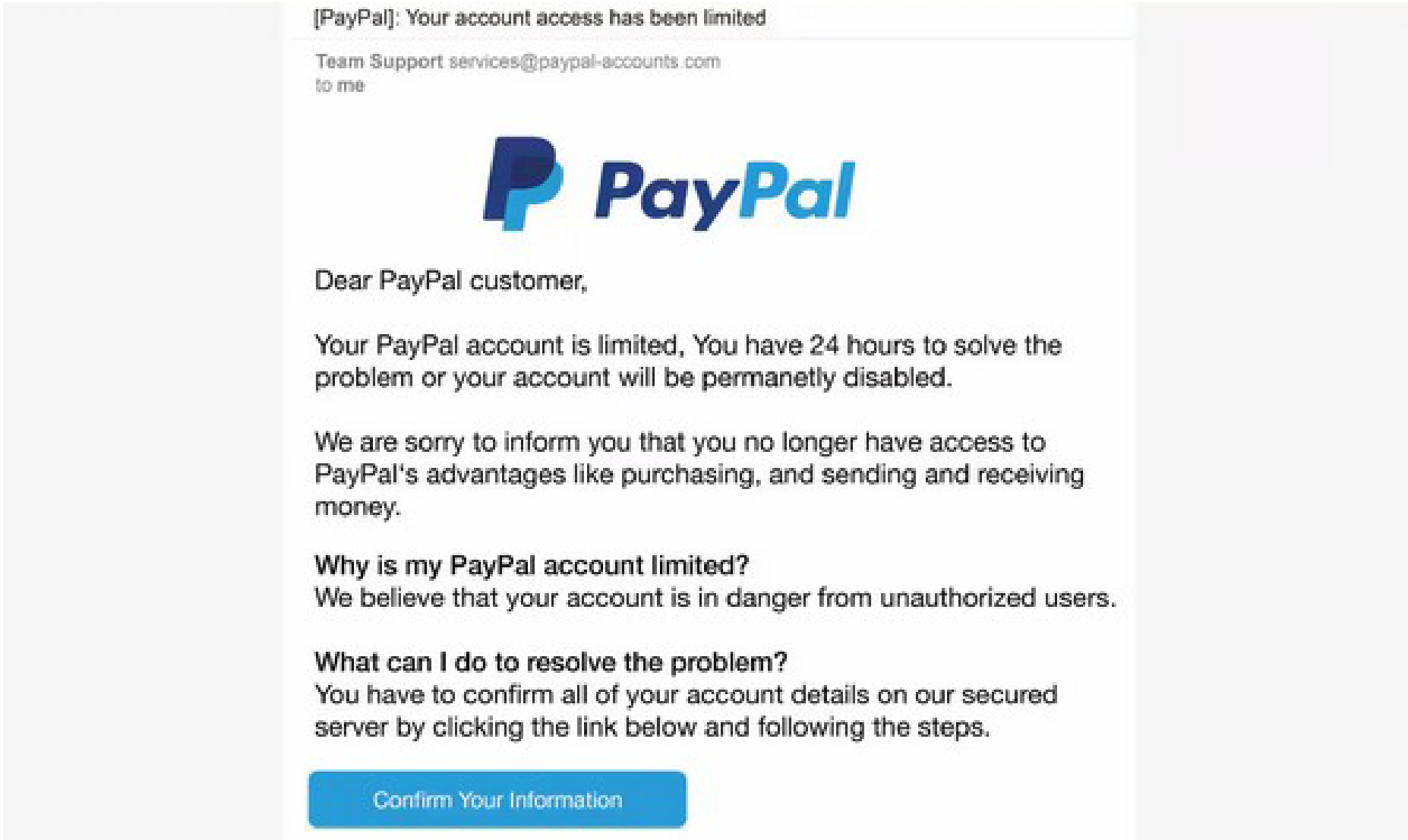
Anatomy of an Email: Red Flags

- Unexpected sender (email doesn't match name)
- Urgent/threatening messages
- Generic greetings (“Dear Customer” or “Dear User”)
- Suspicious links & attachments
- Spelling & grammar mistakes

Spot the Difference

- Urge you to take immediate action to prevent an account from being disabled or deleted.
- Ask you to reset a compromised password or confirm login credentials.
- Include an alert that someone reported you to the administrator.

Spot the Difference: Real Example



[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.

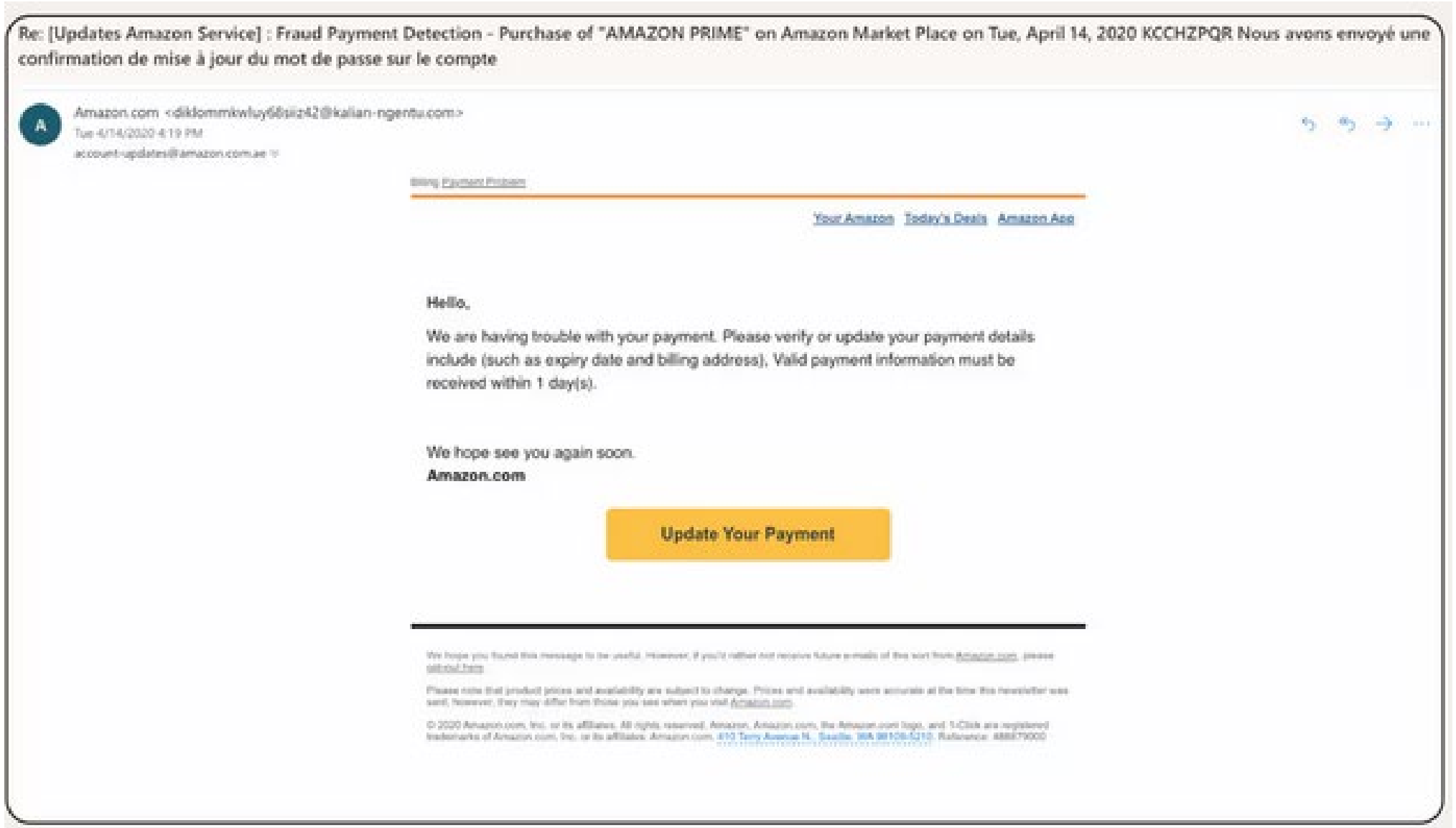
What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

How to tell this is a phishing email:

- The user’s name hasn’t been specified and it’s a generic greeting. The first sentence provokes a sense of urgency, hoping the user acts without thinking. There are also grammar and spelling errors in the email if you look closely.

Spot the Difference: Real Example



How to tell this is a phishing email:

- This Amazon phishing email comes from a suspicious email address, doesn’t include the customer’s name, and pressures the customer to update their payment information quickly.

Subject: Action Required: Microsoft Account Password Update

From: Microsoft Security Team security-update@microsoft-support.com

Dear User,

Due to recent security enhancements, your account requires verification.

Please update your password by clicking the link below. Failure to comply within 24 hours will result in limited access to your account.

Update Password Now: Click Here

Thank you for helping us keep your account secure.

Microsoft Support Team

Key Red Flags in This Example:

- Urgent or threatening language (“24 hours will result in limited access”)
- Generic greeting (“Dear User”)
- Suspicious sender email address (not a real Microsoft domain)
- A link that does not lead to a legitimate Microsoft site
- Request to update password—classic credential harvesting tactic

Safe Email Practices

- Verify senders & links before clicking
- Never open unknown attachments
- Report suspicious emails to IT
- Never send sensitive info via email
- Use Multi-Factor Authentication (MFA)

Reporting Suspicious Emails

- Don’t reply, click links, or download files
- Report immediately to IT
- Delete the email after reporting

Office Reminders

- Lock your screen when you leave your desk or system
- Win + L

- Close all your programs, especially at the end of the day

Your Role in Company Security

- Treat every email as a risk
- Protect all sensitive info
- Report security concerns right away

Quick Quiz

- CEO asks for gift cards: What do you do?
- True/False: It's safe to click a link from someone you know
- Received an unexpected invoice email: Next steps?

Other Cybersecurity Safety Tips

- Be alert – never pick up unknow USB stick
- Lock your devices
- Limit activities on public WI-FI
- Protect personal information
- Screen all phone calls
- Do not reply to unknown text messages
- Do not call
- Freeze Your Credit

Key Takeaways

- Email is the #1 attack method
- Spot red flags
- Verify before you click
- When in doubt, DELETE or ASK