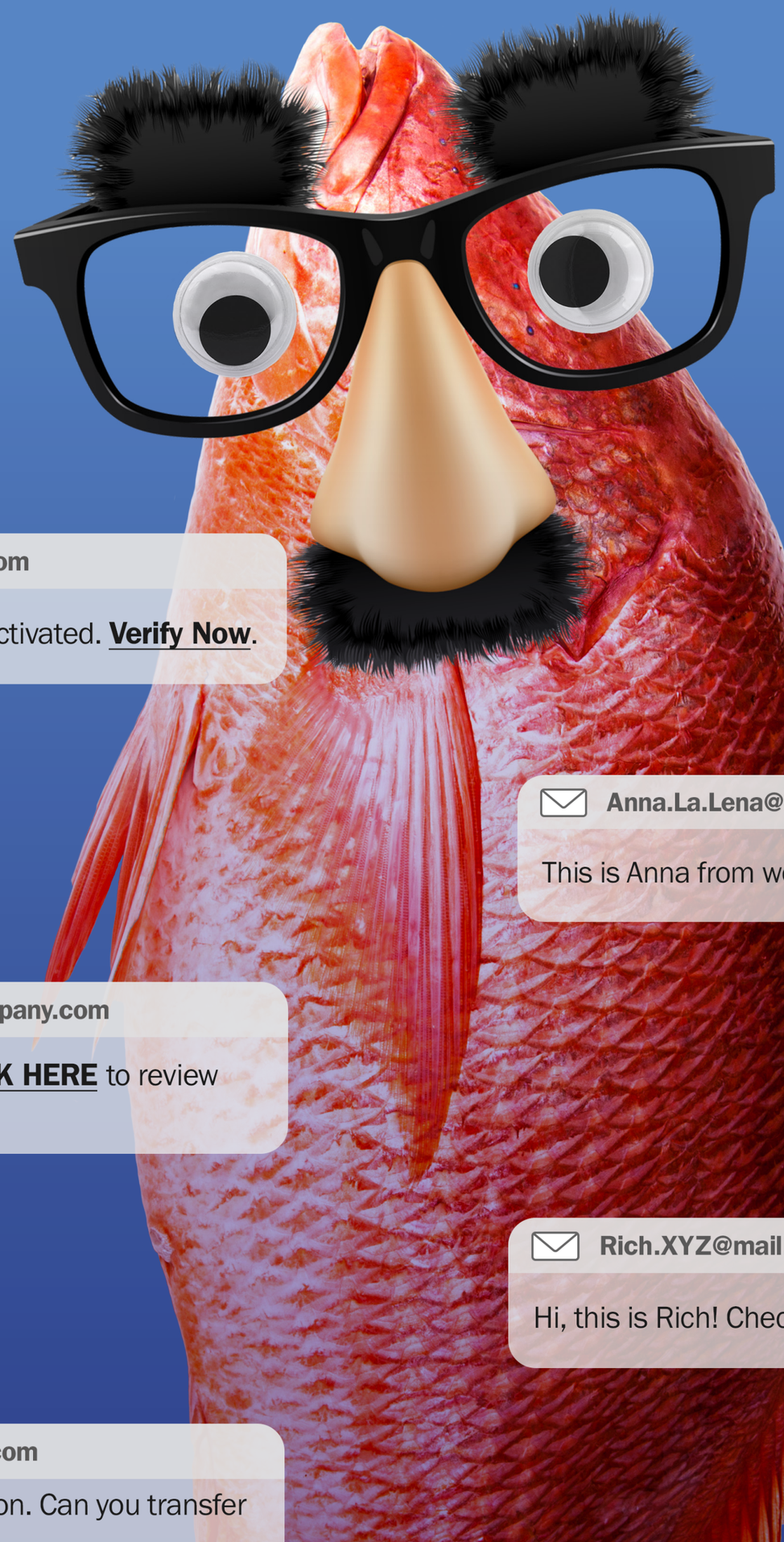

Webmaster@webmail.com

Your account has been deactivated. **Verify Now**.

Anna.La.Lena@business.co

This is Anna from work. Please review **this.**

HumanResources@company.com

This is Carol from HR. **CLICK HERE** to review your pay stub.

Rich.XYZ@mail.com

Hi, this is Rich! Check **this** song out!

Elizabeth.Harper@mail.com

I lost my passport on vacation. Can you transfer money **HERE**?

Does something seem "phishy" to you?

Millions of people are targets of phishing scams each day. Cyber criminals use a variety of tricks to disguise themselves as legitimate companies, your colleagues, and people you would normally trust. Make sure you know who you are really communicating with and be careful of suspicious links.

October is National Cyber Security Awareness Month. For more information and tips to stay safe online, visit: **https://www.dhs.gov/ncsam**

Homeland Security

National Cyber Security Awareness Month

CyberAware

How to Spot a Phishing Scam

Cyber crime is a critical threat with social engineering attacks becoming more sophisticated, realistic, and difficult to recognize. Phishing attacks are one of the most common forms of cyber crime. What does a phishing email look like? Review the example below for characteristics of a phishing scam disguised to look like a legitimate email.

Generic subject line

Legitimate emails usually have detailed subject lines. A vague subject line can be a key indicator of a phishing scam.

Suspicious URL

Hover over links included in emails to see the actual destination of the URL.

Improper use of copyright

Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately:
www.security.webmail.com.

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

Bad grammar/spelling

Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

Unnecessary urgency

Use your intuition and if something 'feels' wrong, consider calling the organization or office directly to validate the email.

Types of Social Engineering

Phishing:

Online communications or emails designed to lure individuals into providing sensitive information.

Tip: When in doubt, throw it out. If an email looks suspicious, contact the organization/individual directly to validate the legitimacy of the email. You can also report the email to your email provider's IT Security department.

Ransomware:

A type of malware that prevents or limits users from accessing their system or select files, unless a ransom is paid to restore access.

Tip: Be proactive and protect against data loss by backing up your files and keeping them safe on a physical, external storage device.

Identity Theft:

An act of wrongfully obtaining and using another person's information that involves fraud or deception.

Tip: Be diligent before posting personal information online and think carefully before sharing information through apps and websites.

For more information and tips to stay safe online throughout the year, visit: https://www.dhs.gov/ncsam

Homeland Security

National Cyber Security Awareness Month

CyberAware