Atlas Communications

European Cyber Security Month Workshops

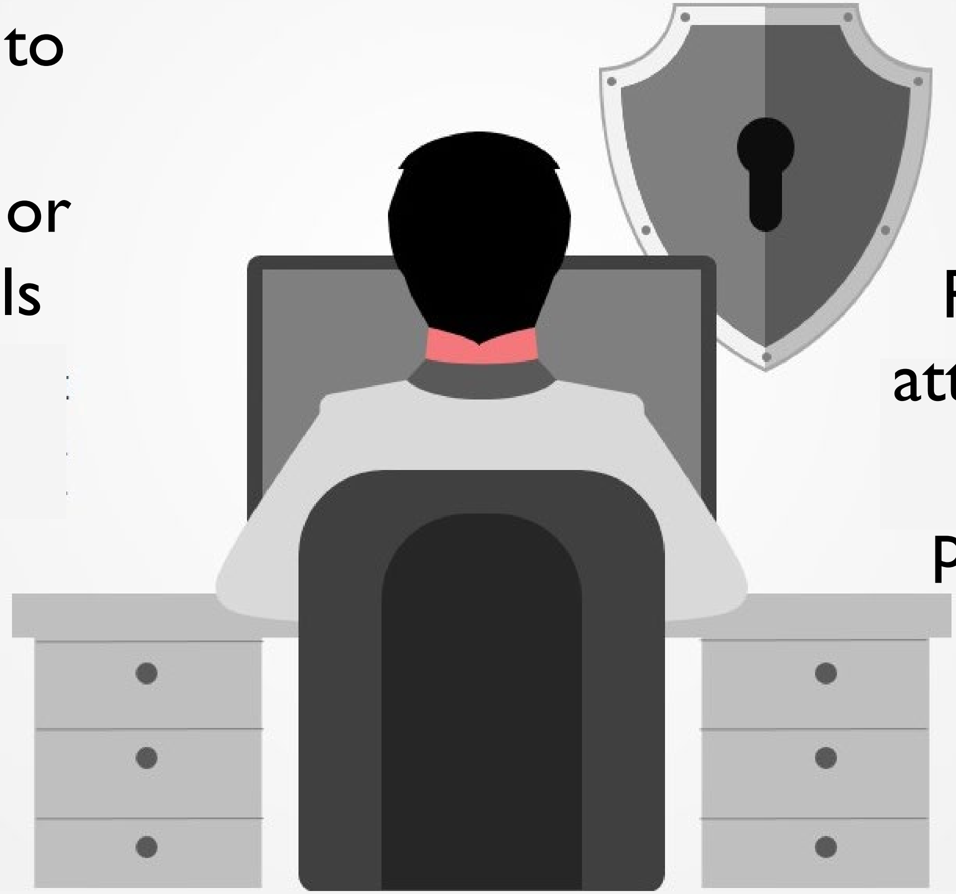
# 1) HOW TO IDENTIFY PHISHING SCAMS AND PROTECT YOUR ORGANISATION

EUROPEAN
CYBER
SECURITY
MONTH

# What is a Phishing Attack?

In a typical phishing attack, scammers send fake emails asking for sensitive information or containing links to bad websites.

They might try to trick you into sending money or steal your details to sell on



Remember, Phishing doesn't attack computers, it attacks the people using the computers

30% of phishing scam emails are opened

ATLAS

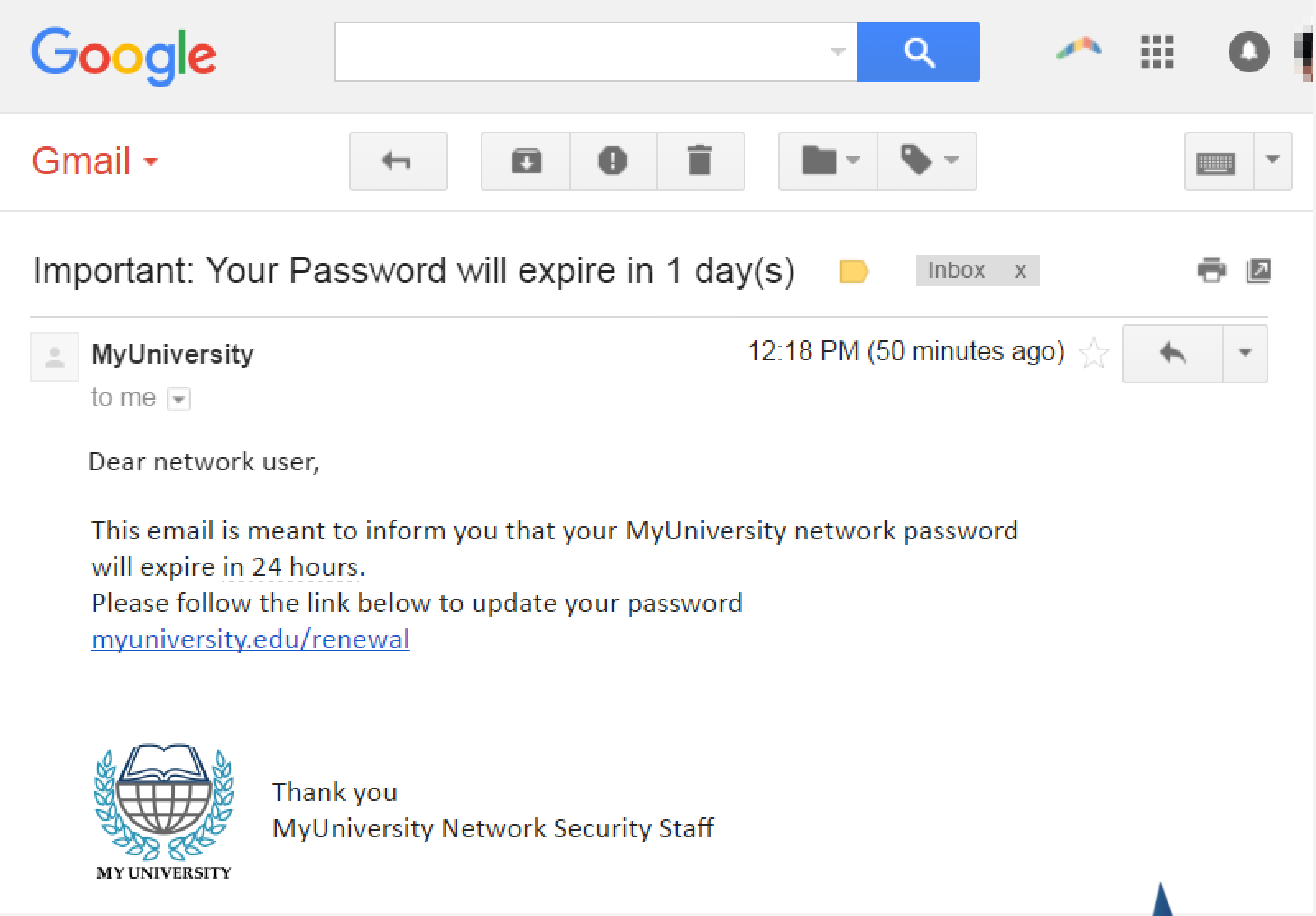
# Types of Phishing Attacks

**Spear Phishing:** A highly targeted form of phishing that hones in on a specific group of individuals or organisations.

**Whaling:** A form of phishing targeted at executive level individuals.

**Cloning:** Whereby a legitimate email is duplicated but, the content is replaced with malicious links or attachments.

# Phishing Examples



Important: Your Password will expire in 1 day(s)

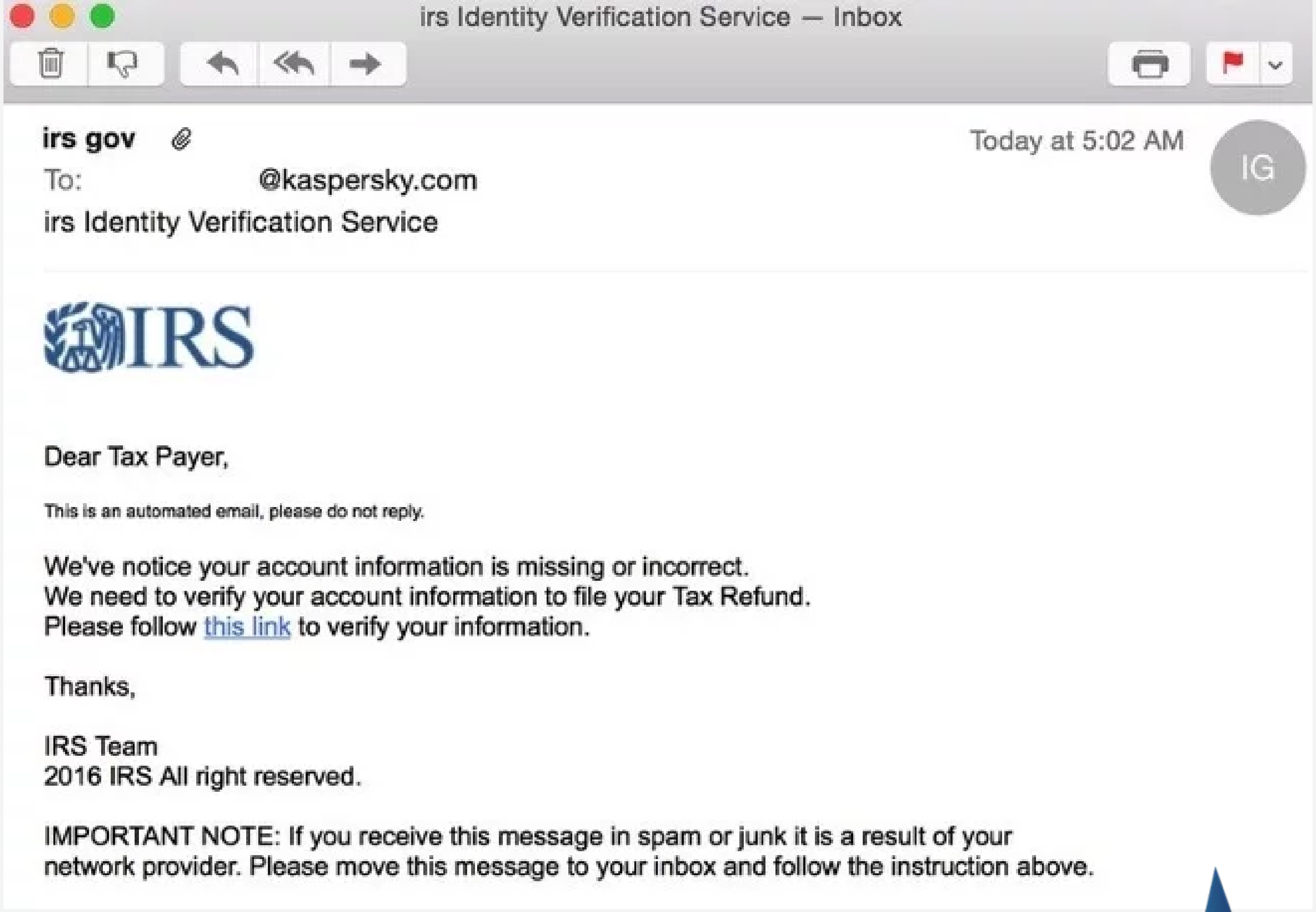
MyUniversity
to me

12:18 PM (50 minutes ago)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff



irs Identity Verification Service — Inbox

**irs gov**

To: @kaspersky.com

irs Identity Verification Service

Today at 5:02 AM

IRS

Dear Tax Payer,

This is an automated email, please do not reply.

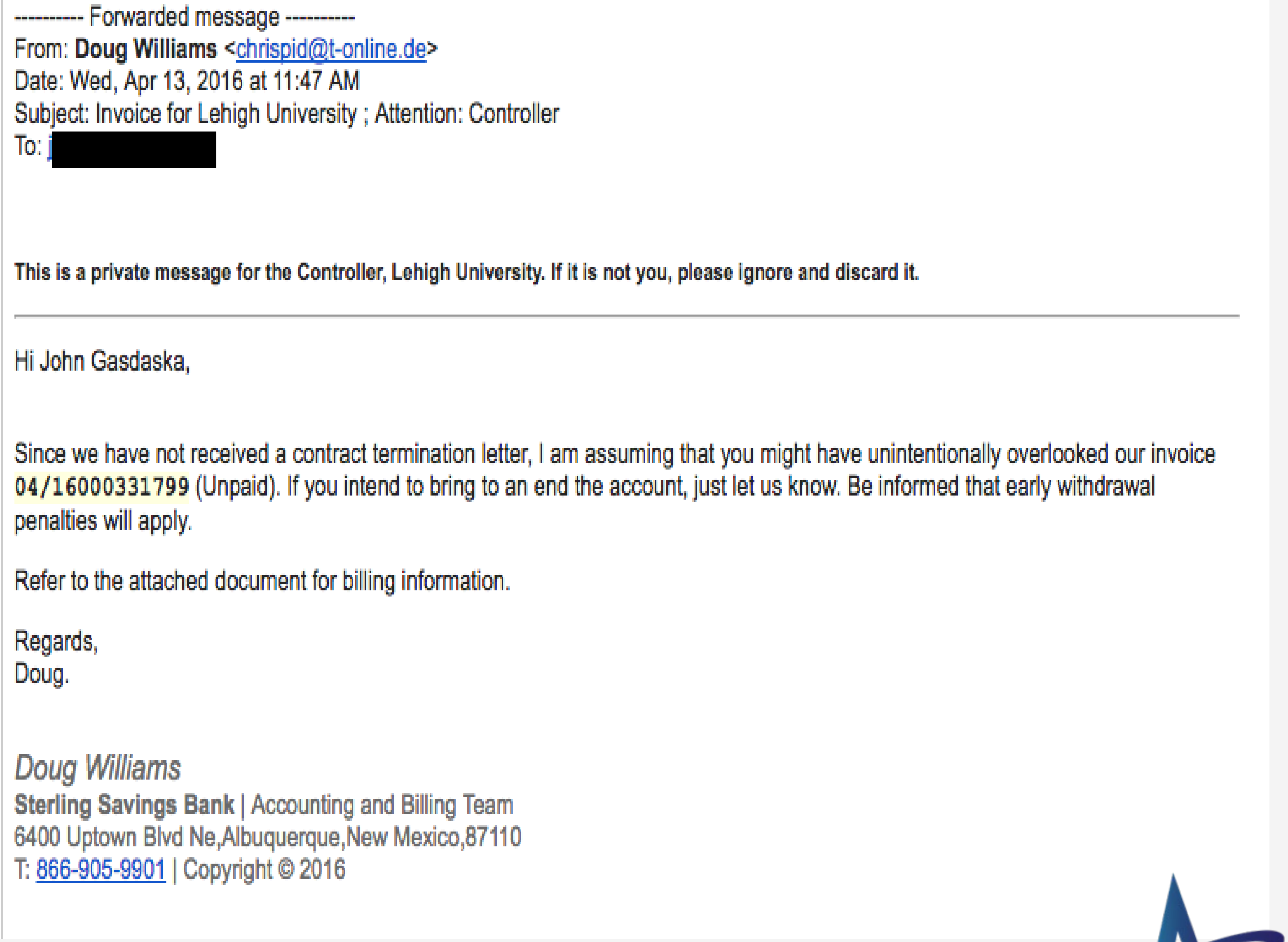
We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow this link to verify your information.

Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.

ATLAS



---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: [redacted]

**This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.**

Hi John Gasdaska,

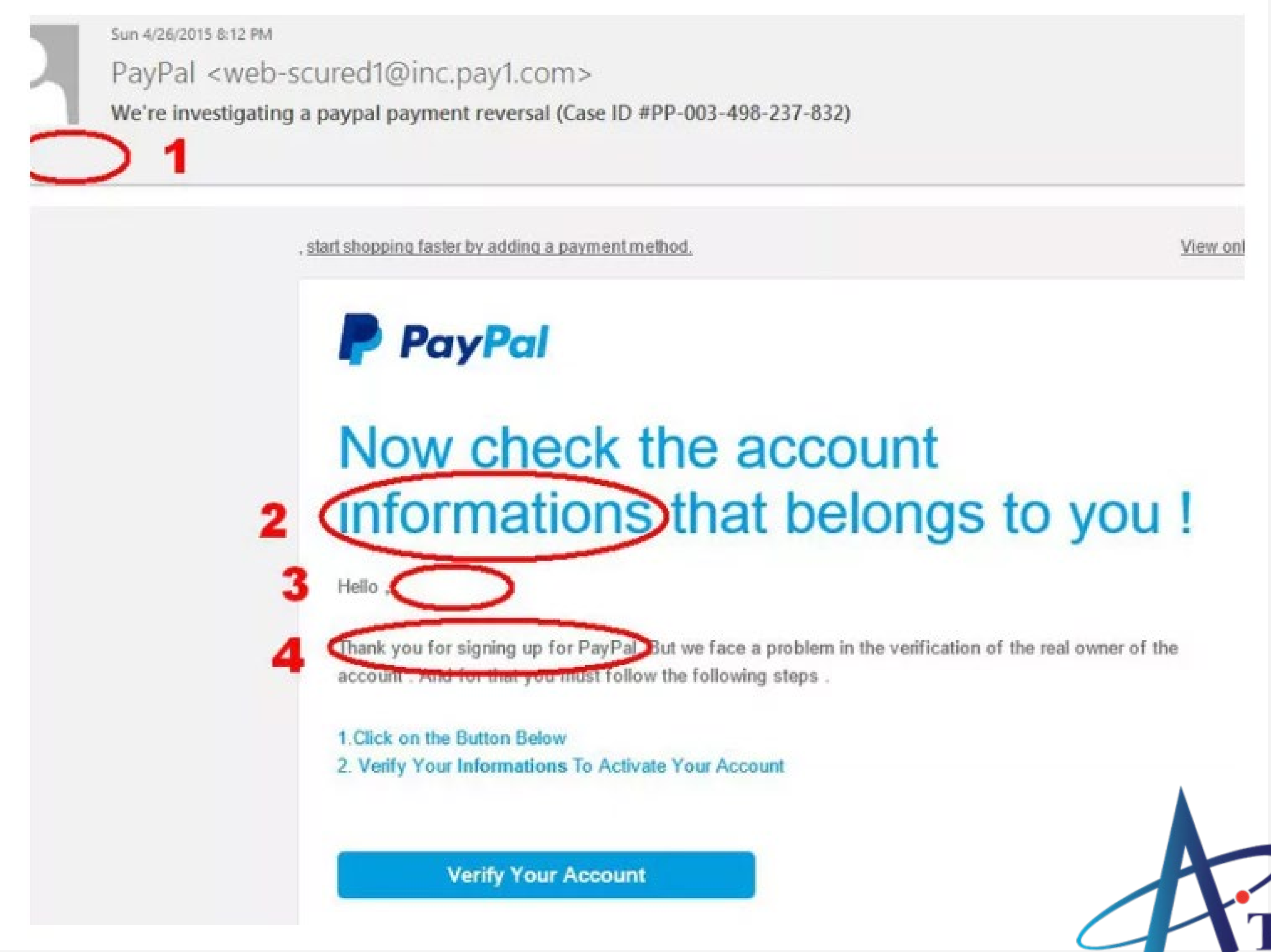
Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice 04/16000331799 (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

*Doug Williams*
**Sterling Savings Bank** | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016

# How to Spot a Phishing Email



Sun 4/26/2015 8:12 PM

PayPal <web-scured1@inc.pay1.com>

We're investigating a paypal payment reversal (Case ID #PP-003-498-237-832)

, start shopping faster by adding a payment method.

View onl

Now check the account informations that belongs to you !

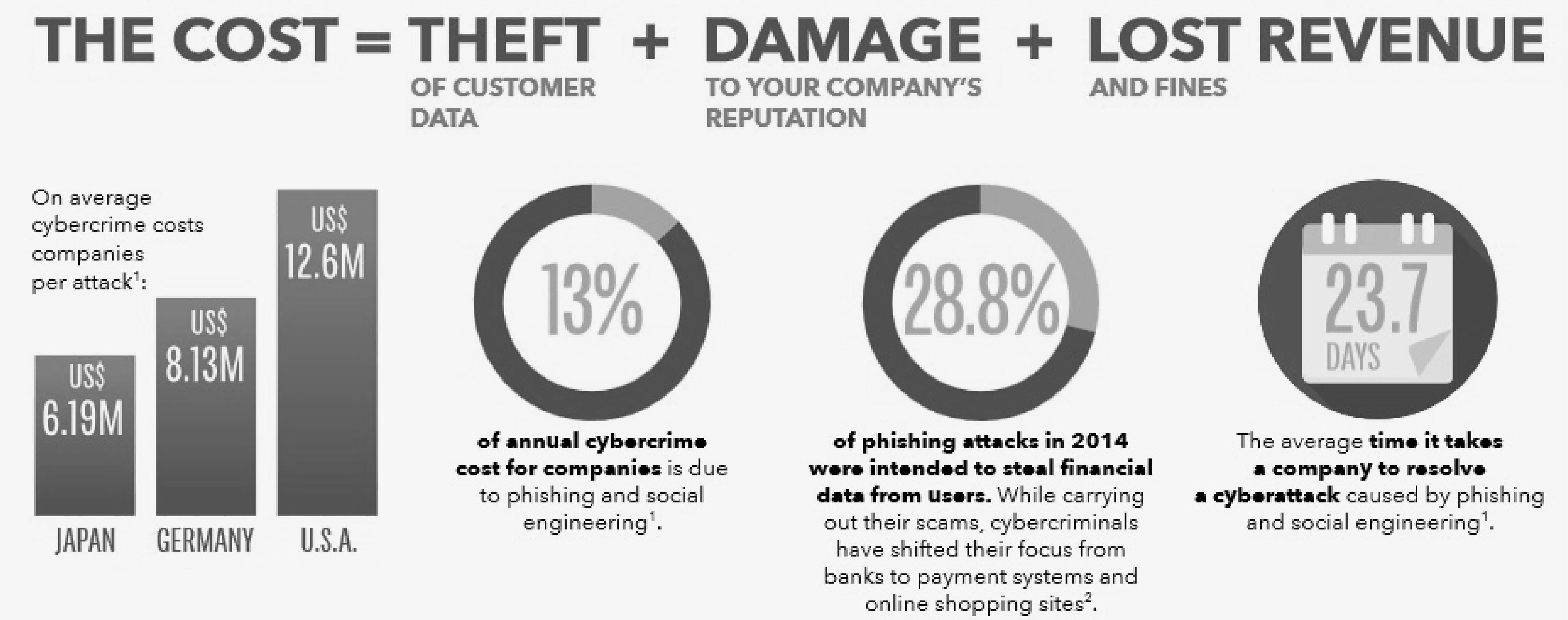
Hello ,

Thank you for signing up for PayPal. But we face a problem in the verification of the real owner of the account . And for that you must follow the following steps .

1.Click on the Button Below
2. Verify Your Informations To Activate Your Account

ATLAS

# Effects of Phishing on Businesses



**THE COST = THEFT** OF CUSTOMER DATA **+ DAMAGE** TO YOUR COMPANY'S REPUTATION **+ LOST REVENUE** AND FINES

On average cybercrime costs companies per attack[1]:

**13% of annual cybercrime cost for companies** is due to phishing and social engineering[1].

**28.8% of phishing attacks in 2014 were intended to steal financial data from users.** While carrying out their scams, cybercriminals have shifted their focus from banks to payment systems and online shopping sites[2].

**23.7 DAYS** The average **time it takes a company to resolve a cyberattack** caused by phishing and social engineering[1].

# Protecting yourself from Phishing

Check for obvious signs of phishing like poor spelling & grammar. Does the senders email address look legitimate, or is it trying to mimic someone you know?

Ask yourself whether someone impersonating an important individual via email should be challenged or have their identity verified before action is taken.

Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact if an attack is successful.

# Atlas Communications
# European Cyber Security Month Workshops

**Let everyone know that your business is promoting cyber security awareness by tweeting @AtlasComms using #PoweredByAtlas**

EUROPEAN
CYBER
SECURITY
MONTH