MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami

CSIRT.SK
WWW.CSIRT.GOV.SK

CS DANUBE

Computer Security Incident Response Team Slovakia CSIRT.SK

Martin Jurčík, CSIRT.SK

CS Danube, 15th March, 2016, Prague

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DANUBE REGION strategy START
Danube Region Project Fund

How to recognize a phishing?

Martin Jurčík, CSIRT.SK

CS Danube, 15th March, 2016, Prague

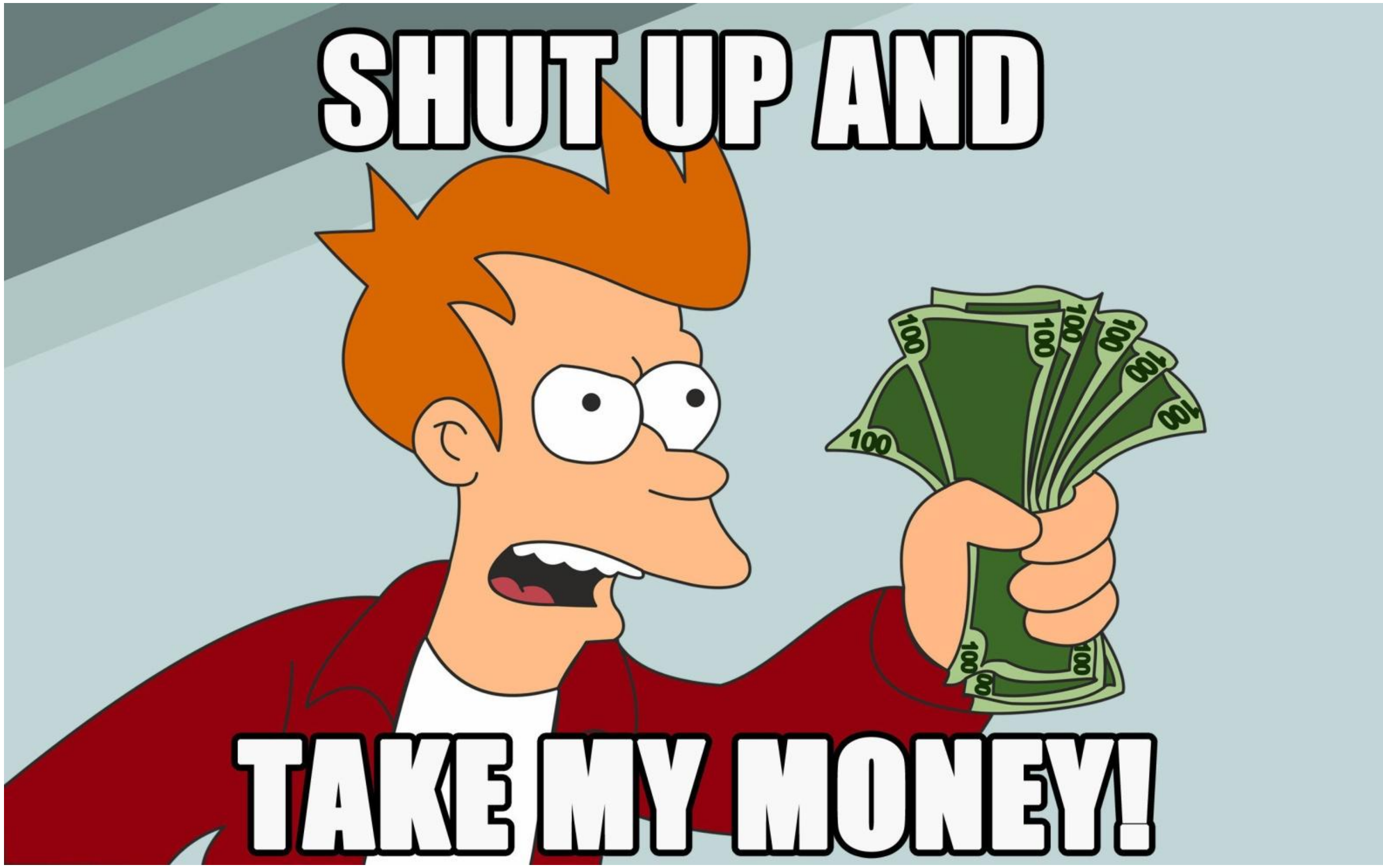
CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Agenda

1. **Phishing**
2. **Case study**
3. **Summary**

Phishing

- **Scam** - an attempt to defraud a person or group by gaining their confidence
- **Phishing** - the attempt to acquire sensitive information such as usernames, passwords, and credit card details



Phishing

- Do you know Mr. Abacha Tunde?

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

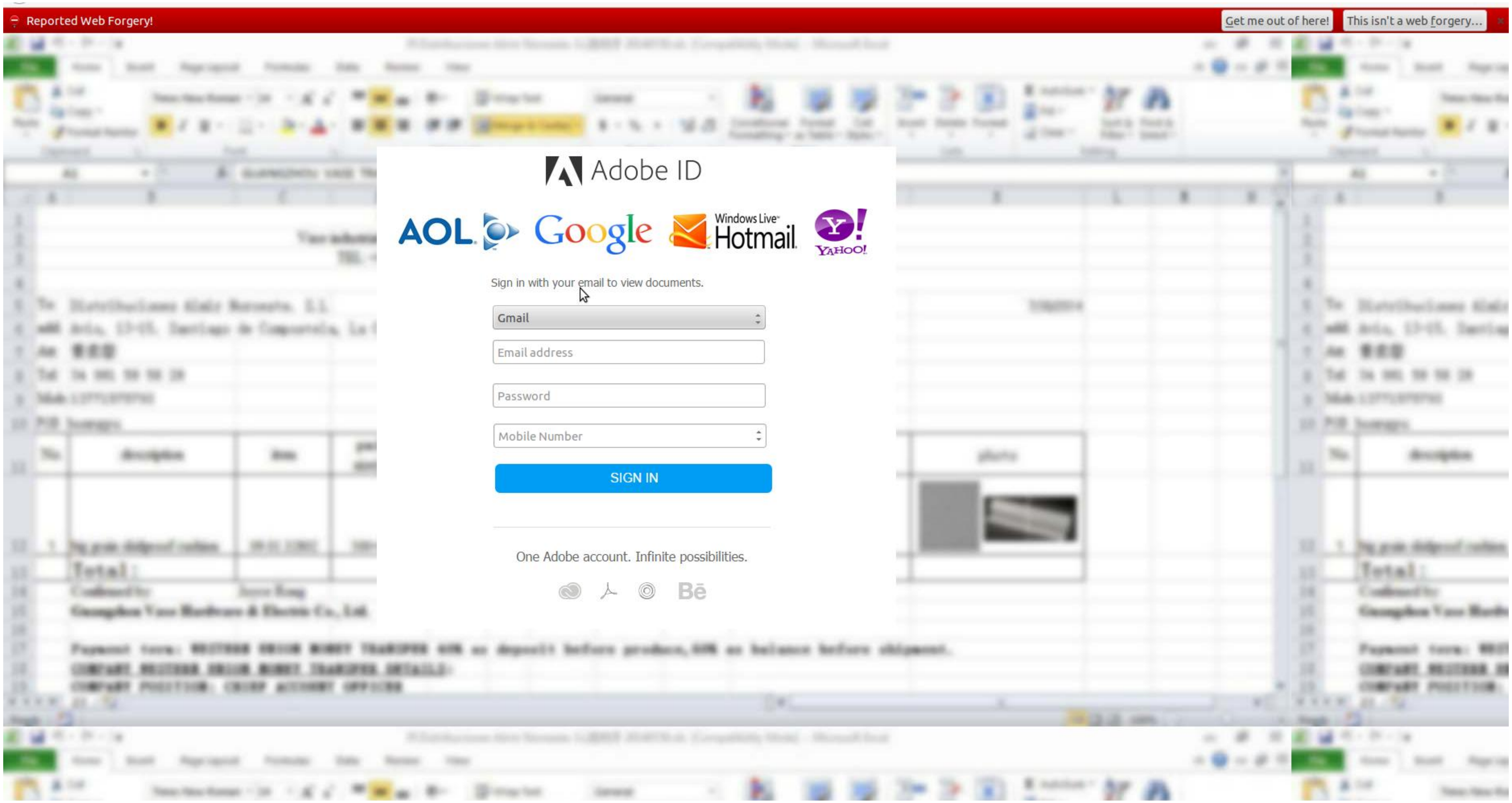
I am Dr. Bakare Tunde, the cousin of **Nigerian Astronaut, Air Force Major Abacha Tunde**. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names. Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Phishing

- Example



Reported Web Forgery!

Adobe ID

Sign in with your email to view documents.

Gmail

Email address

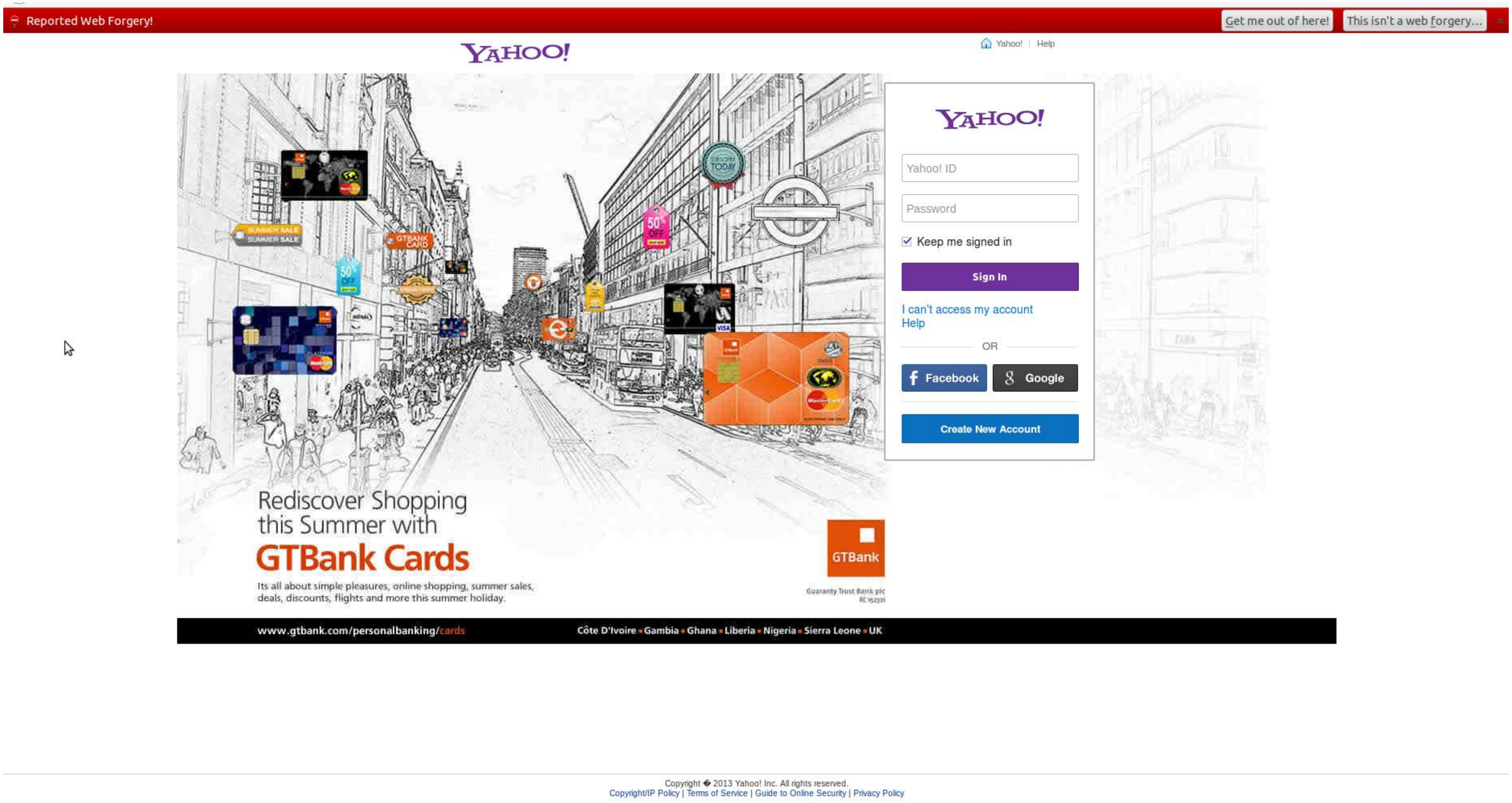
Password

Mobile Number

One Adobe account. Infinite possibilities.

Phishing

- Example



Reported Web Forgery!

Get me out of here! | This isn't a web forgery...

YAHOO!

Yahoo! | Help

Rediscover Shopping
this Summer with
GTBank Cards

Its all about simple pleasures, online shopping, summer sales,
deals, discounts, flights and more this summer holiday.

GTBank

Guaranty Trust Bank plc
RC 152321

www.gtbank.com/personalbanking/cards

Côte D'Ivoire • Gambia • Ghana • Liberia • Nigeria • Sierra Leone • UK

YAHOO!

Yahoo! ID

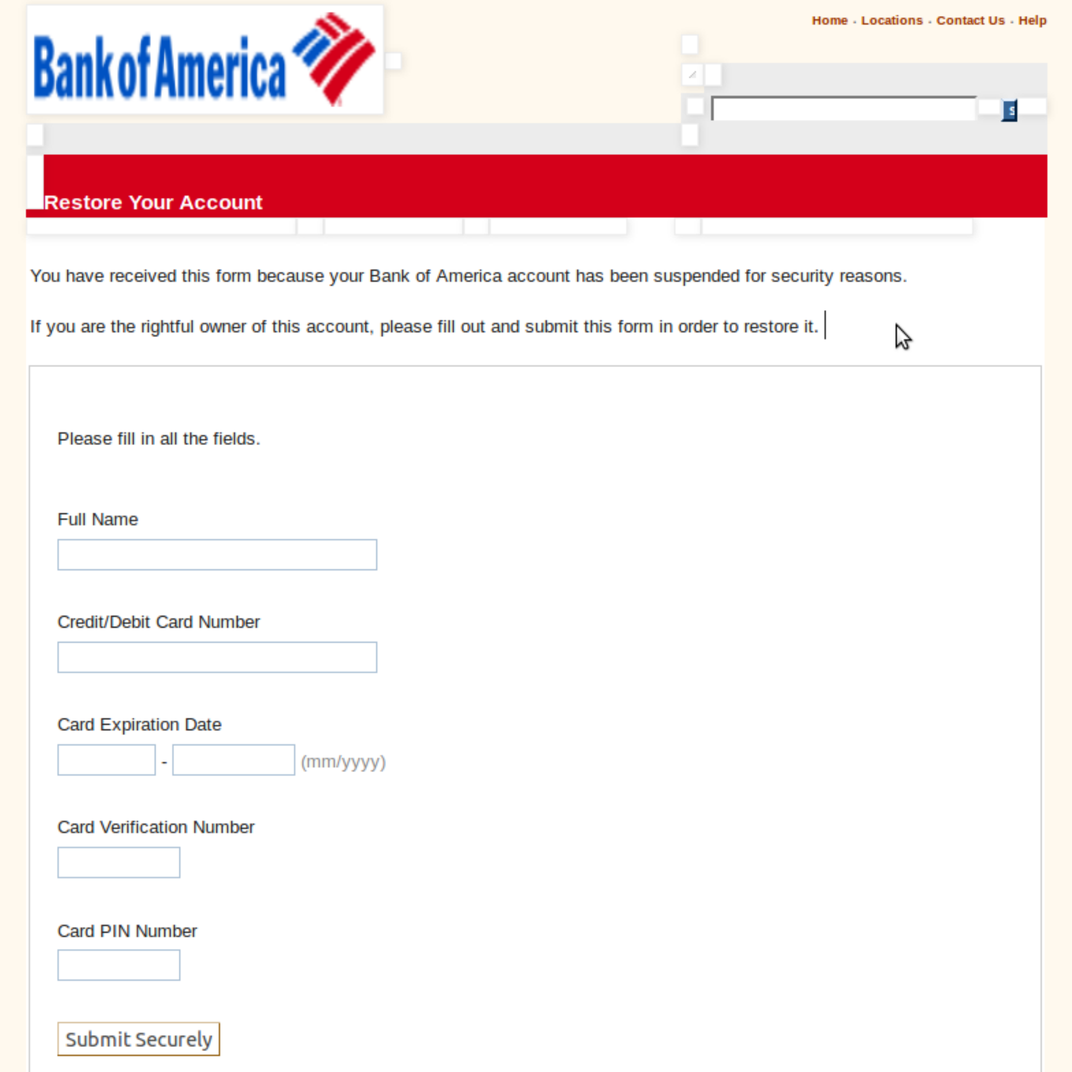
Password

☑ Keep me signed in

Copyright � 2013 Yahoo! Inc. All rights reserved.
Copyright/IP Policy | Terms of Service | Guide to Online Security | Privacy Policy

Phishing

- Example



Restore Your Account

You have received this form because your Bank of America account has been suspended for security reasons.

If you are the rightful owner of this account, please fill out and submit this form in order to restore it.

Please fill in all the fields.

Full Name

Credit/Debit Card Number

Card Expiration Date

- (mm/yyyy)

Card Verification Number

Card PIN Number

Phishing

How to recognize a phishing?

- Check email sender
- Check email form
  - Number of recipients
  - Analyze the salutation
  - Review the signature
- Check for spelling mistakes
- Check URL links in email body
- Beware of urgent or threatening language in the subject
- Beware of emails asking for banking information
- Do not provide personal information
- Do not believe everything you see

Case Study

Phishing from Fisheries

From: Mail Delivery System <fisheries@moa.gov.jm>

==

Subject: Please respond to info

Hello Web Email User,

This is an automatic warning message That your mailbox is at capacity. The system has denied you from sending or receiving any messages because your email account was logged in from a different location.

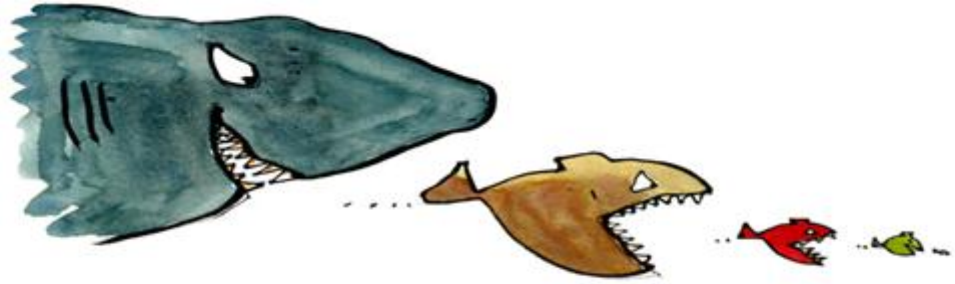
To increase your current mailbox size so that new messages could arrive and to reset your account on the server;

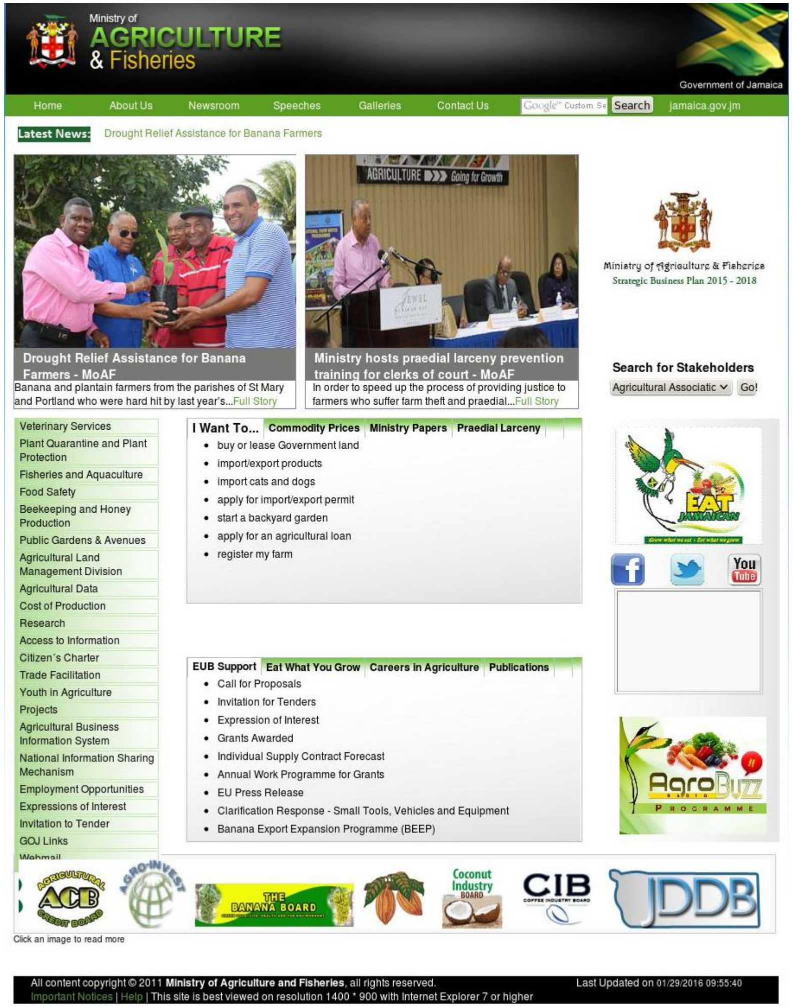
Please Fill the Form Below;
Email Address:
User ID:
Password:

Thank you for using the Online Web Email!

ADMIN TEAM.

This email has been checked for viruses by Avast antivirus software.
https://www.avast.com/antivirus





Latest News: Drought Relief Assistance for Banana Farmers

Drought Relief Assistance for Banana Farmers - MoAF
Banana and plantain farmers from the parishes of St Mary and Portland who were hard hit by last year's...Full Story

Ministry hosts praedial larceny prevention training for clerks of court - MoAF
In order to speed up the process of providing justice to farmers who suffer farm theft and praedial...Full Story

I Want To... | **Commodity Prices** | **Ministry Papers** | **Praedial Larceny**

- buy or lease Government land
- import/export products
- import cats and dogs
- apply for import/export permit
- start a backyard garden
- apply for an agricultural loan
- register my farm

EUB Support | **Eat What You Grow** | **Careers in Agriculture** | **Publications**

- Call for Proposals
- Invitation for Tenders
- Expression of Interest
- Grants Awarded
- Individual Supply Contract Forecast
- Annual Work Programme for Grants
- EU Press Release
- Clarification Response - Small Tools, Vehicles and Equipment
- Banana Export Expansion Programme (BEEP)

Click an image to read more

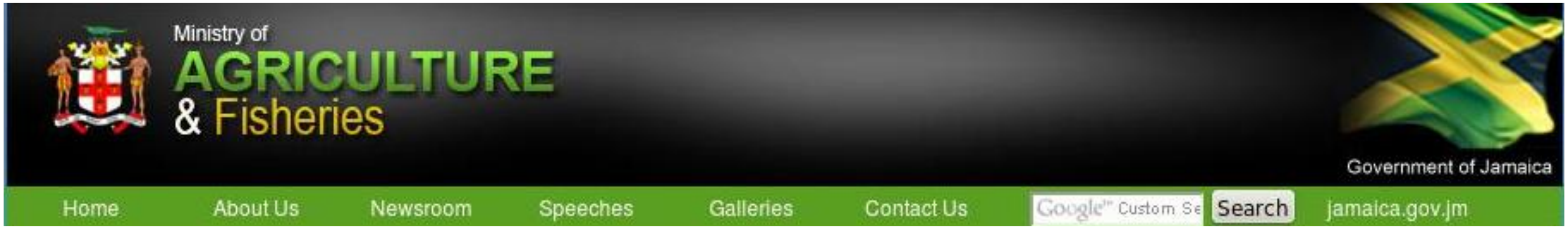
All content copyright © 2011 **Ministry of Agriculture and Fisheries**, all rights reserved.   Last Updated on 01/29/2016 09:55:40
Important Notices | Help | This site is best viewed on resolution 1400 * 900 with Internet Explorer 7 or higher

MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami

CSIRT.SK
WWW.CSIRT.GOV.SK

Case Study



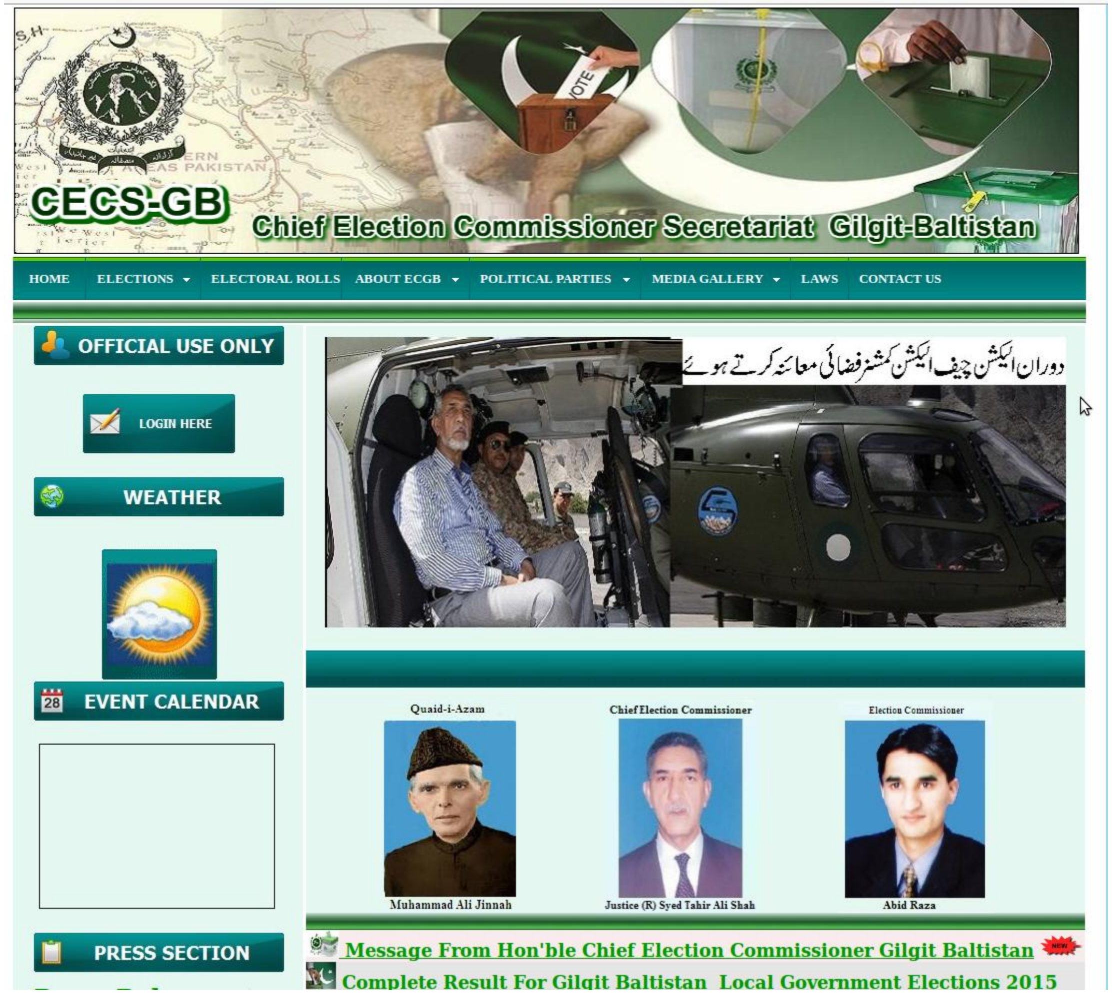
```
Received: from mail.datacentrum.sk ([192.168.32.6]) by DCDC2.dcnet.dacenba.sk (HF384)
Subject: [SPAM] WARNING
Received: from unknown (HELO g2inmail.gov.sk) ([100.64.16.30]) by mail.datacentrum.sk with ESMTP; 28 Jan 2016 11:09:21 +0100
Authentication-Results: mail.gov.sk; dkim=none (message not signed) header.i=none; spf=None smtp.mailfrom=fisheries@moa.gov.jm; spf=None smtp.helo=postmaster@MAW2K8SRV08.moa.gov.jm
Received: from unknown (HELO MAW2K8SRV08.moa.gov.jm) ([208.163.40.132]) by mail.gov.sk with ESMTP/TLS/AES128-SHA; 28 Jan 2016 11:09:21 +0100
Received: from userPC (41.71.217.239) by MAW2K8SRV08.moa.gov.jm (10.0.251.8) with Microsoft SMTP Server id 14.1.355.2; Thu, 28 Jan 2016 05:08:03 -0500
Reply-To: <info@ecgb.gov.pk>
From: Mail Delivery System <fisheries@moa.gov.jm>
To: Mail Delivery System <fisheries@moa.gov.jm>
Date: Thu, 28 Jan 2016 11:07:39 +0100
Message-ID: <003c01d159b3$e82f3140$b88d93c0$@gov.jm>
MIME-Version: 1.0
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AdFZs7XFIz+LBPdHQL+ngnhIOz1ROw==
Return-Path: fisheries@moa.gov.jm
X-Originating-IP: [41.71.217.239]
X-Notes-Item: E03E83F0:B761F2CF-5EE44D0E:55E2467E;
 type=4; name=$INetOrig
```

41.71.217.239
Nigeria (Visafone Communications Limited)

208.163.40.132
Jamaica (Cable & Wireless Jamaica)

Case Study

- **ecgb.gov.pk**



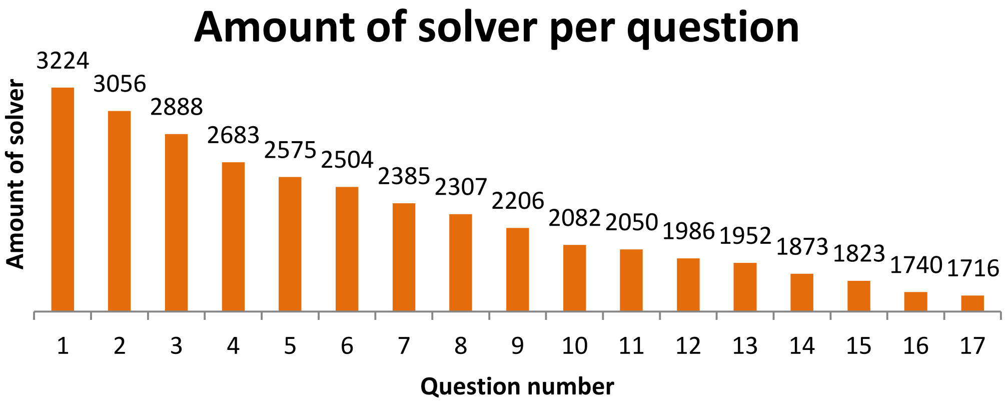
Message From Hon'ble Chief Election Commissioner Gilgit Baltistan

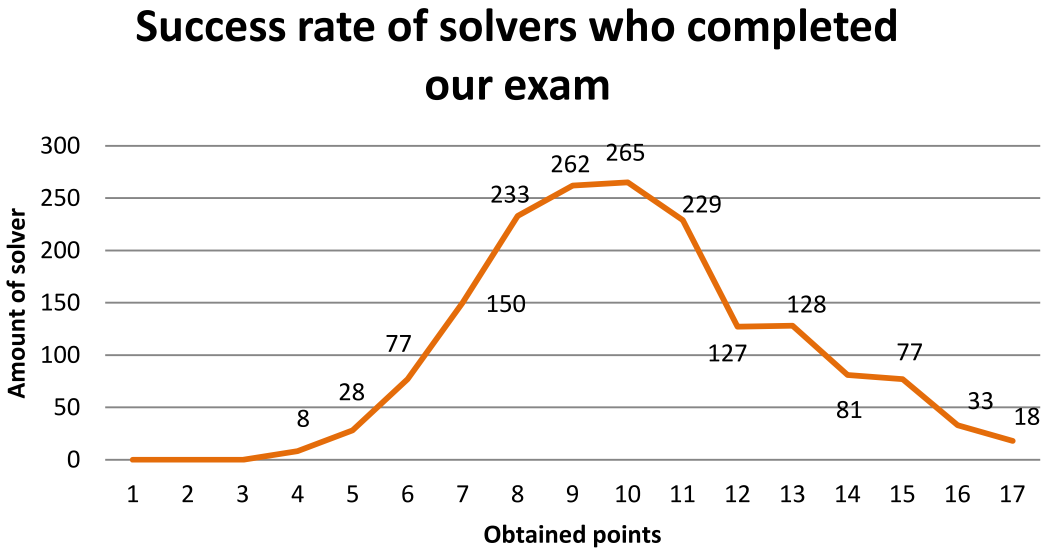
Complete Result For Gilgit Baltistan Local Government Elections 2015

Summary

Our own phishing test

- 17 questions
- Chuck Norris (chucknorris@gmail.sk)
- Legitimate or fraudulent ?

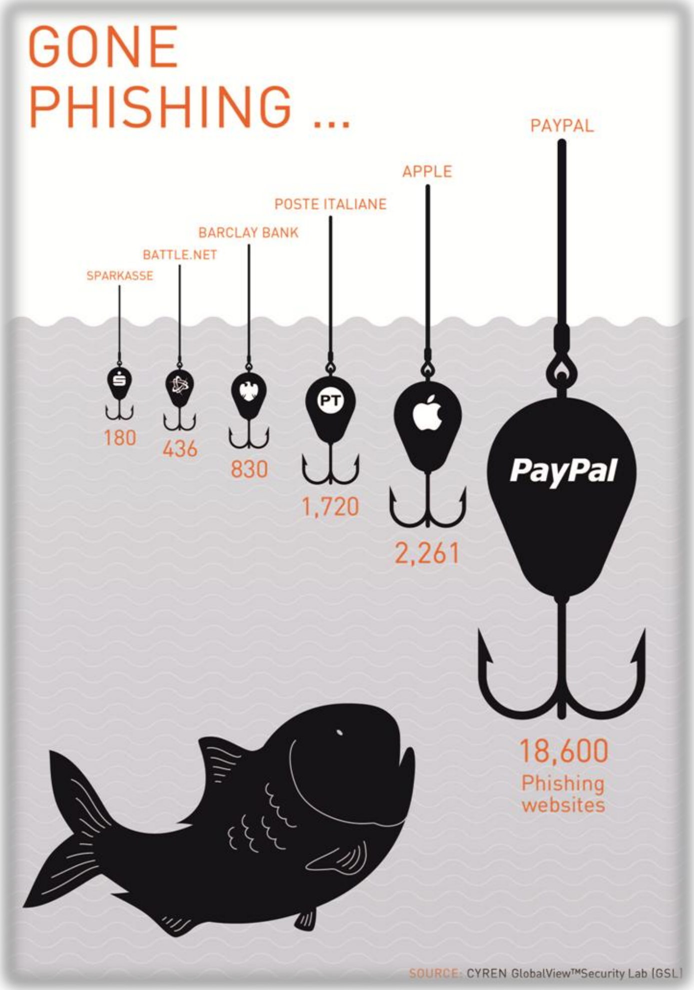




Summary

All examples and one special on:

http://tinyurl.com/csdanube



SOURCE: CYREN GlobalView™Security Lab (GSL)

Thank you for your attention!

MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami

CSIRT.SK
WWW.CSIRT.GOV.SK

CS DANUBE

Thank you for your attention!

CSIRT.SK
DataCentrum
Cintorínska 5, 814 88 Bratislava
www.csirt.gov.sk
Telephone: +421 2 59 278 205, +421 2 59 278 454
Contact: info@csirt.gov.sk
Incident report: incident@csirt.gov.sk

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DANUBE REGION strategy START
Danube Region Project Fund