

Don't Get Caught in the Phishing Net

Dan Goldsmith

Introduction

About me

- Dr. Daniel Goldsmith
- Senior Lecture: Ethical Hacking and Cyber Security

Ethical Hacking

- Study of Cyber Security
- Lots of interesting technical challenges to solve
- Look for flaws in systems and propose fixes
- Adversarial Mindset

The IOC

- UK Wide initiative to increase Technology skills
- 20 UK universities involved
- Coventry University Leads focus on Industry
- <https://instituteofcoding.org/>

Phishing

Definition

Phishing is a form of social engineering, where targets are contacted by someone posing as a legitimate entity, in an attempt to get them to provide sensitive information.

Definition

- A Phishing attack will generally attempt do one of two things:
 - Get the user to hand over sensitive details that can be used in a later crime or attack
 - Get the user to install malware, to compromise the users machine.

A Brief History

- As old as the Con Trick
- Current technique Became prevalent in the 1990's with the early WWW
 - AOHell automated some parts of the attack

Early AOL Email Example

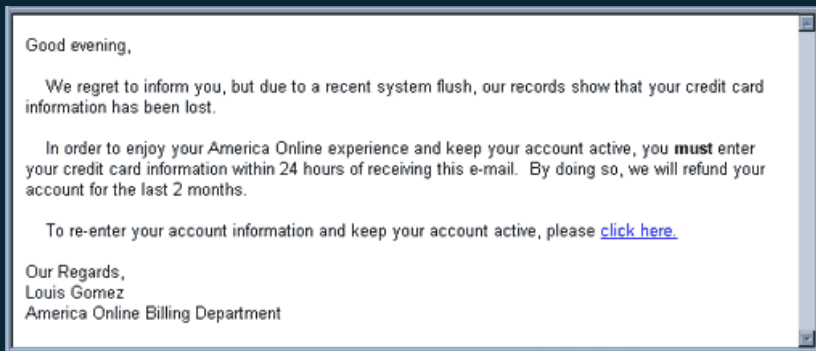


Figure 1: AOL Email Example

The "Classic" 419 Scam

From: Columns [info@qnet.com]
Sent: 21 November 2011 01:18
Subject: 20:11:2011

Good day,

I am Johnson Ahmad, a close confidant of the daughter of the late Colonel Muammar Gadhafi. I am a financial analyst based here in the United Kingdom. If you are conversant with what is going on in the World, you would have heard that Colonel Muammar Gadhafi has being killed. Presently the United Nations is doing everything in their power to ensure that all the family funds stashed in different banks all over the World are confiscated, of which they have succeeded 100%. As a close confidant and Financial adviser to the daughter of the late Libyan leader, i am privy to a secret deposit amounting to Sixteen million British pounds sterling (216,000,000). These funds is deposited with a financial firm. This is the only deposited funds that has not being confiscated by the United Nations due to the fact that it was deposited with the name of one of her maid and personal assistant. But due to the current investigation going on and the nature of things surrounding the Gadhafi family presently, it is unsafe and unwi

This is the reason i am sending you this email on behalf of the daughter of the late Libyan leader, Ayeesha, to help receive this funds in your name as the depositor and owner of the funds. If you are willing to help out please do reply back to this mail as soon as you can, as time is of a great excess, before the funds is discovered.

As soon as i get a response from you, i will give you full details on what needs to be done to achieve it. Ayeesha would not mind how much percentage you would want for your help and assistance provided the deposit is changed to your name and that it remains in your custody until the whole investigation dies off as this money is the last hope for her to live a normal life.

I will be expecting to hear from you.

Johnson Ahmad.

419 Scam

- Named after relevant section of Nigerian Penal Code
- Origin Nigeria in early 2000's.
- One of the most recognisable Phishing attempts
 - FBI estimates it Still costs Millions to economy (2018) ¹

¹[<https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud>]

I Love You



Figure 3: I Love You

I Love you

- First automated spam.
- Estimated 45 Million Infections within 5 days
- Estimated cost \$5-8 Billion

First Prosecution

- 2004 Federal Trade Commission filed first Lawsuit
- 17 Year old Californian
- Spoofing AOL website to harvest credentials.

Phishing in the Modern World

These times are (Not) changing

- Same basic method of attack
- Delivered via:
 - Email
 - Social Media
 - Phone (Vishing)
 - SMS (Smishing)
 - TypoSquatting

Phishing Statistics

- Spam is about 45% of all email sent (14.5 Billion Per day)
- About 45,000 phishing campaigns a month
- Estimated cost of \$20 Billion per year.

Phishing Success Rates

- 30% of phishing emails opened by target
 - 12% click on the link
- Cause of around half of all data breaches

Phishing and Corona Virus

- Reported 600% increase in number of phishing attempts
- Hackers moved quickly to exploit the situation
 - Fear, Uncertainty, and Doubt
 - Increase in home working

Modern Phishing

- Basic Premise hasn't changed.
 - 419 Scam
 - Credential Harvesting
 - Malware delivery

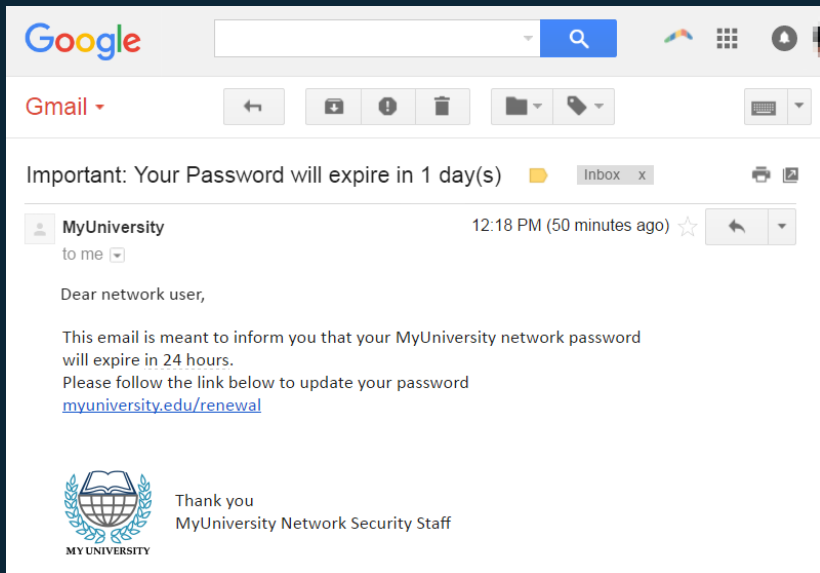
Types of Phishing

- Moved on from the Trawler approach
 - Spear Phishing
 - Whale Phishing

Spear Phishing

- Target an individual (or group of individual)
- Personalised details to increase authenticity
- Decreases number of targets but increases chance of success

Spear Phishing



The screenshot shows a Gmail interface with a search bar at the top. Below the search bar, the Gmail logo and navigation icons are visible. The main content area displays an email with the subject "Important: Your Password will expire in 1 day(s)". The email is from "MyUniversity" and is addressed "to me". The body of the email reads: "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". At the bottom of the email, there is a logo for "MY UNIVERSITY" and the text "Thank you MyUniversity Network Security Staff".

Google

Gmail

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

MyUniversity 12:18 PM (50 minutes ago)

to me

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

Figure 4: Spear Phishing

Whale Phishing

- Subset of Spear Phishing
- Target C Level
 - High value target. Rewards for success much greater.


Phishing Cookbook

Create a sense of urgency.

- Motivates user to *ACT NOW*
 - Time limited offer
 - Penalties if you don't act
- Pressure can make target more prone to error

Sense of Urgency

From: **Costco Shipping Agent** <manager@cbcbuilding.com> Hide
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>



Unfortunately the delivery of your order [COS-0077945599](#) was cancelled since the specified address of the recipient was not correct. You are recommended to complete [this form](#) and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

Figure 5: Urgency

Sense of Urgency

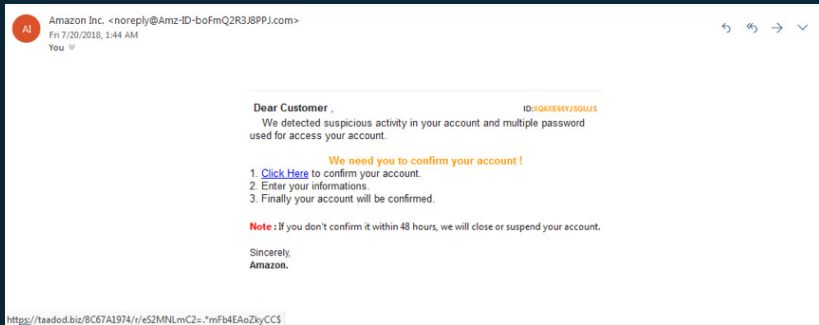


Figure 6: Amazon

Pretend to be a trusted source.

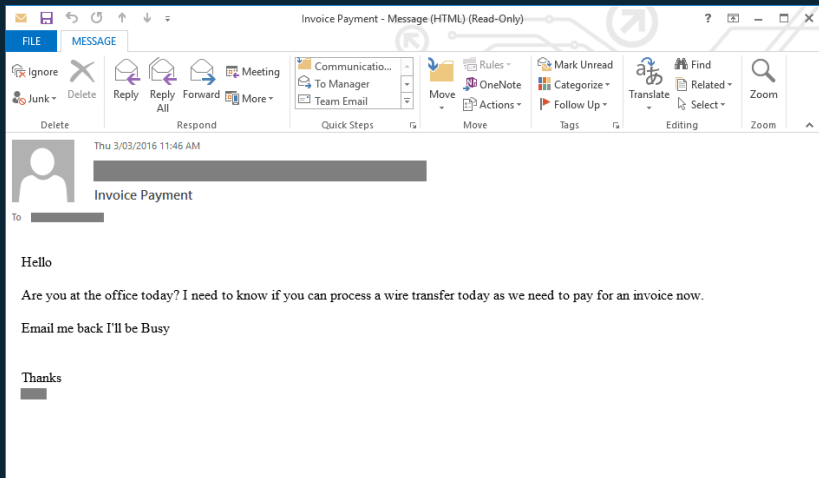


Figure 7: Trusted Source

Pretend to be in authority.

- Combines both of the approaches
 - Threatening action to be taken
 - Get target to trust the source.

Tips to Spot Phishing



Your Transaction Was Declined

Dear customer,

We are sorry, Your recent PayPal transaction was declined because your account has been limited until we hear from you. In just 3 easy steps, you'll be back to shopping securely and conveniently again.
So, update now!

[Click To Update](#)

Update Your Account ??? [Update Now](#)

[Help Center](#) [Partner Directory](#) [Logo Center](#) [Security](#) [Business Center](#)

Check the URL

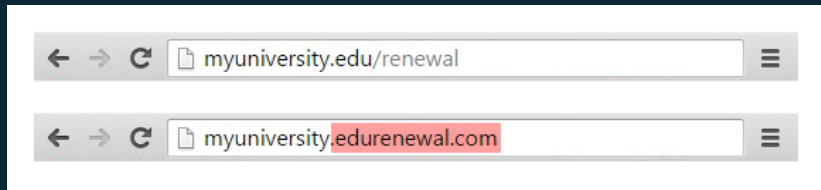


Figure 9: URL

Check the URL

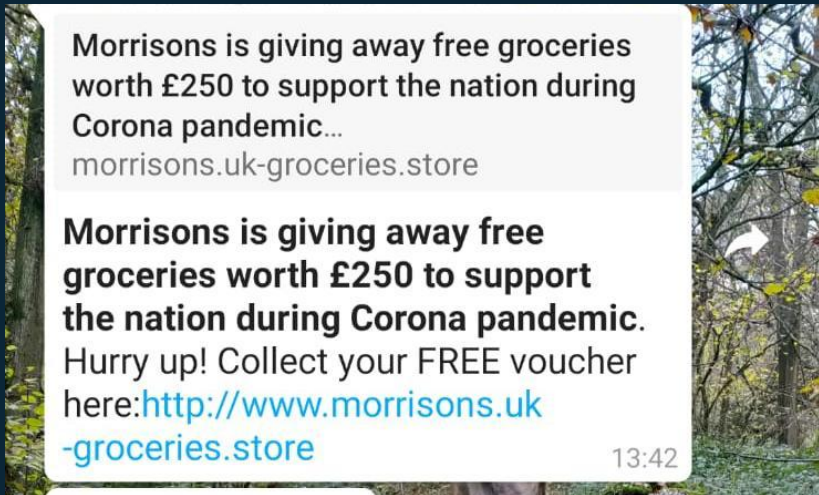


Figure 10: Text Message

More Suspicious Links

File Edit View Go Message Tools Help

From NETFLIX <member@netflix.ssl.com>
Subject Your Netflix Membership is on hold Date Thu, 19 Apr 2018 14:41 UTC

Reply Reply All Forward More

NETFLIX <http://interweb-billing9.com/membershipkey=1847758831894800264859937456/>

Validation failed

During a routine check of your account we have failed to validate the billing method we have on record for your account.

To continue using the Netflix service you will need to validate your billing information.

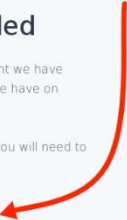
[CONTINUE >>](#)

Your current membership status is to remain on hold until this process is completed.

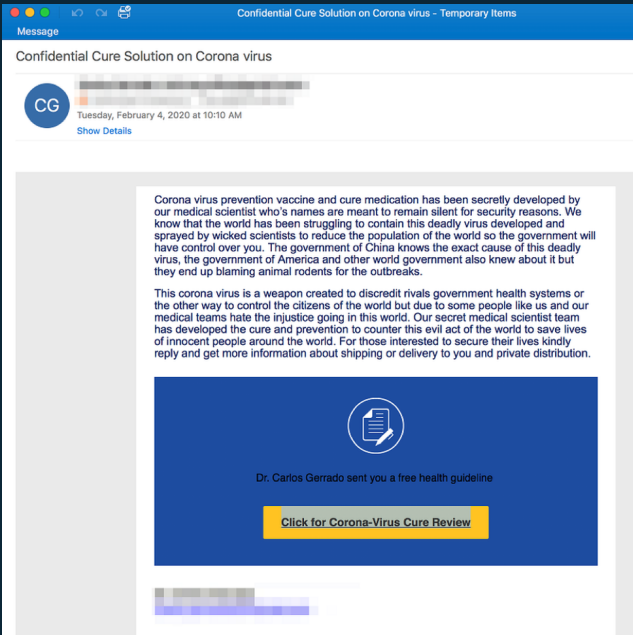
Netflix Billing Support

TWEET LIKE FORWARD

Preferences | Unsubscribe



Are you Expecting the Email




The image shows a screenshot of an email client interface. At the top, there are window control buttons (red, yellow, green) and a search icon. The title bar reads "Confidential Cure Solution on Corona virus - Temporary Items". Below this, the word "Message" is displayed. The main header of the email is "Confidential Cure Solution on Corona virus". A circular profile picture with the initials "CG" is shown next to a redacted sender name. The timestamp is "Tuesday, February 4, 2020 at 10:10 AM" with a "Show Details" link below it. The email body contains two paragraphs of text. The first paragraph discusses the secret development of a vaccine and cure for Corona virus, mentioning the government of China and the government of America. The second paragraph describes the virus as a weapon and mentions a secret medical scientist team. At the bottom of the email body, there is a blue call-to-action box with a document icon and the text "Dr. Carlos Gerrado sent you a free health guideline". A yellow button with the text "Click for Corona-Virus Cure Review" is positioned below the text. At the very bottom of the screenshot, there is a redacted area with a purple gradient.

Confidential Cure Solution on Corona virus - Temporary Items

Message


Confidential Cure Solution on Corona virus

 [Redacted Name]

Tuesday, February 4, 2020 at 10:10 AM
[Show Details](#)

Corona virus prevention vaccine and cure medication has been secretly developed by our medical scientist who's names are meant to remain silent for security reasons. We know that the world has been struggling to contain this deadly virus developed and sprayed by wicked scientists to reduce the population of the world so the government will have control over you. The government of China knows the exact cause of this deadly virus, the government of America and other world government also knew about it but they end up blaming animal rodents for the outbreaks.

This corona virus is a weapon created to discredit rivals government health systems or the other way to control the citizens of the world but due to some people like us and our medical teams hate the injustice going in this world. Our secret medical scientist team has developed the cure and prevention to counter this evil act of the world to save lives of innocent people around the world. For those interested to secure their lives kindly reply and get more information about shipping or delivery to you and private distribution.



Dr. Carlos Gerrado sent you a free health guideline

[Click for Corona-Virus Cure Review](#)

[Redacted Area]

Protecting against it

Accept that the Spam filter wont save you

- Trusting *ANY* software to protect you is a mistake
- Its relatively easy to send an email as someone else
- Effectiveness of filter relies on a set of Rules

The Padlock wont save you

- The padlock means the site is HTTP's
- Communication is encrypted
- However huge rise in HTTPS based phishing sites (40%)

HTTPS Spoofed Website

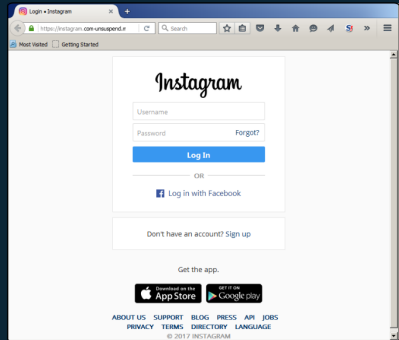
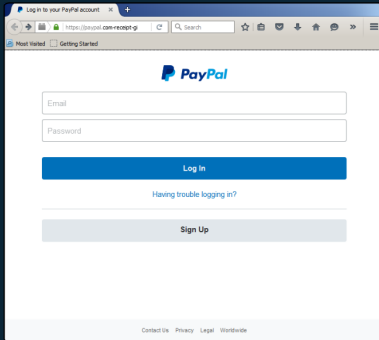


Figure 13: Paypal

Trust your Gut

- Does something not feel right about
- We can be good at spotting when something isn't right.
 - Contact organisation directly

Coronavirus Related Phishing

New programme against COVID-19



<GOV UK Notify>



The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund (rebate)* of 128.34 GBP.

[Access your funds now](#)

The funds can be used to protect yourself against COVID-19(
<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

----- Forwarded message -----

From: GOV UK Notify <danielnhs@pinkcontract.com>

To: "

Sent: Friday, 6 March 2020, 08:28:50 GMT

Subject: UK Updates on COVID-19



The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund (rebate)* of 128.34 GBP.

[Access your funds now](#)

[The funds can be used to protect yourself against COVID-19(
<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.



Claim Your Refund

The screenshot shows a web browser window with the URL `jrkJjiri.com.cn/admin/edit/Dialog/tax.gov.uk/start-process.htm`. The page header includes the HM Revenue & Customs logo and navigation links for Home, Contact HMRC, and Help. The main heading is "Claim your refund online". Below this, there is a note: "*Indicates required information" and "Please use this form to claim your tax refund amount of 275.31 GBP." The form is titled "Enter your details" and contains several input fields: "First name: *", "Last name: *", "Date of birth dd/mm/yyyy: *" (with three separate boxes for day, month, and year), "Address: *", "Town: *", "Postcode: *", "Phone: *", and "Mother's maiden name: *". A red instruction states: "Please verify your official identity by confirming your mother's maiden name." Below this is a section titled "Registered payment account" with fields for "Card number: *" and "Expiry date: *" (with a note "For example, 03 2019").

HM Revenue & Customs Home Contact HMRC Help

Claim your refund online

*Indicates required information
Please use this form to claim your tax refund amount of 275.31 GBP.

Enter your details

First name: *

Last name: *

Date of birth dd/mm/yyyy: *

Address: *

Town: *

Postcode: *

Phone: *

Please verify your official identity by confirming your mother's maiden name.

Mother's maiden name: *

Registered payment account

Card number: *

Expiry date: *

For example, 03 2019



Figure 16: Claim your Refund

WHO has a message for you

Coronavirus (2019 -nCoV) Safety Measures - Temporary Items


Message

Coronavirus (2019 -nCoV) Safety Measures

  @who-pc.com

Tuesday, February 4, 2020 at 7:08 PM

[Show Details](#)

 CoronaVirus_Safety...
1.6 MB

[Download All](#) [Preview All](#)

Dear Sir/Madam,


Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards



General Internist
Intensive Care Physician
WHO Plague Prevention & Control

Donations in Bitcoin

↩ Ответить

↩↩ Ответить всем

➔ Переслать

Больше ▾

От Corona Support <info@[REDACTED].com> ☆

Тема **CDC HEALTH emergency coronavirus (2019-nCoV) Network** 10:49

Обратный адрес info@[REDACTED].com ☆

Кому tom0184@[REDACTED].tw ☆

Dear Sir/Madam

The center for disease control and Prevention (CDC) continues to work to go all out to control an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China, that began in December 2019. Updated list of new case around your city are available at www.cdc.gov/coronavirus/2019.

CDC has established an incident management system to co-ordinate a domestic and international public health response to check mate this virus. Funding of the above project is quite a huge costs and we plead for your good will donation, nothing is too small. From \$10 to any amount

This e-plate form is for timely intervention due to holiday extension of our public Institute/ banks not working, it is really affecting us but together, we must stop the virus! All our research groups have been working round the clock to find a vaccine

Please kindly find our Bitcoin account detail below for your donation and support.

17iiciHtCDFQmEpdmhJ43DtnkGvWgjiXVm

Thanks you for your goodwill contribution in standing against this virus, you are a hero. Please help us share this message to reach as many as possible.

Sincerely

Bitcoin Login

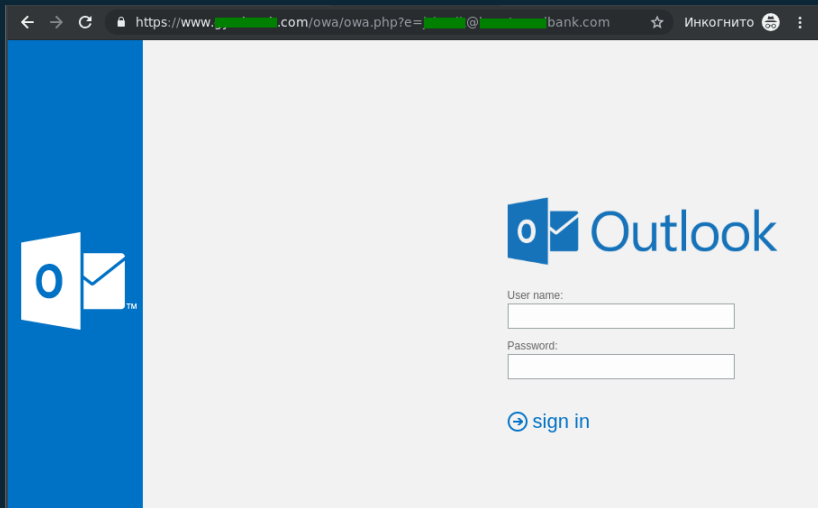


Figure 19: LoginScreen

[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward PDC To Manager Team Email Move Tags Editing Speech Zoom Insights Report Phishing

[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission

CDC INFO <CDC-Covid19@cdc.gov> Wed 2/26/2020 12:00 PM

To [REDACTED]

As you know, the Department of Health and Human Services has declared the Coronavirus (COVID-19) a public health emergency.

At this time, three new cases have been confirmed around your location today. The risk to the Public in your city and throughout the World is very HIGH.

The World Health Organization has named the new coronavirus, Covid-19, and the Centers for Disease Control and Prevention has established precautions.

- * The CDC requires you to avoid (HIGH-RISK) zone around your city to Minimize Chances for Exposures.
- * A high-risk person is currently being monitored around your city center.

For additional information about high-risk places around [https://healing-yui223.com/cd.php?e=\[REDACTED\]](https://healing-yui223.com/cd.php?e=[REDACTED])
Click or tap to follow link.

<https://www.cdc.gov/COVID-19/newcases/feb26/your-city.html>

Figure 20: CDC



Text Messages



Figure 22: Text Messages

Closing Stuff

Next Steps

- Take a Phishing Quiz
 - <https://phishingquiz.withgoogle.com/>
- If you are part of an organisation consider training for staff
 - Cyber Essentials course
 - Pentest companies, Phishing campaign

What happens if I have been Phished

- Don't Panic
- Report to Action Fraud
 - <https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime>
- Change your passwords

Thank you

- Thanks for Listening
- Any Questions?
- Survey Link <https://tinyurl.com/loC-Webinar-April>