Configuration Manual

Using Phishing Simulation Testing to Analyse and Improve Efficacy of Security Awareness Training

MSc Research Project
MSc in Cybersecurity

Caroline Smyth
Student ID: 23183951

School of Computing
National College of Ireland

Supervisor: Dr. Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Caroline Smyth……………………………………………………………………………………

Student ID: 23183951………………………………………………………………………………………..……

Programme: MSc in Cybersecurity……………………………… **Year:** Sept. 23-24

Module: Internship…………………………………………………………………………………….………

Lecturer: Dr. Raza Ul Mustafa………………………………………………………………….………

Submission Due Date: 2/9/24……………………………………………………………………………….………

Project Title: Using Phishing Simulation Testing to Analyse and Improve Efficacy of Security Awareness Training

Word Count: …2002…………….. **Page Count:** …12…………………………….…….………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ………

Date: ……9/9/24…………………………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Caroline Smyth
Student ID: 23183951

1 Introduction

This thesis project is based on data from the KnowBe4 Security Awareness platform[1], of which user, training and phishing simulation test data has been exported. This configuration manual details:

- Software and hardware used in this project
- Setup for a phishing simulation test in KnowBe4 including test setup and ensuring that test emails aren't blocked by email gateway defence systems.
- Export of reports containing current active users, their training history, and their phishing simulation history
- Code:
  - Processing of data including ensuring user history under other email addresses was included, anonymisation of user data
  - Collation of data for each user
  - Analysis of data for each user

Sample CSV files are included for testing the data processing code. CSV files containing anonymised data used in the project are included, and collation and analysis scripts can be run directly on them. CSV type files containing this information in the same format as that given by KnowBe4 can be processed with this code also.

This configuration manual includes the software and hardware configuration used for the creation, processing and analysis of this research.

2 System Configuration

All tasks were completed using a Microsoft Surface laptop with system specification as in Table I.

Table I: Hardware Specifications

Item	Specification
Model	Surface Pro 8
OS Name	Microsoft Windows 11 Pro
Version	10.0.22631 Build 22631

[1] https://www.knowbe4.com

Processor	11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz, 2995 Mhz, 4 Core(s), 8 Logical Processor(s)
Installed Physical Memory (RAM)	16.0 GB

Administrator access to the management console[2] of the KnowBe4 platform is required to create phishing and training campaigns, and to export data from those campaigns, and for users on the system.

Table II: Software Specifications

Software Name	**Version**
Anaconda IDE	MSC v.1916 64 bit (AMD64)
Jupyter Notebook	6.5.4
Kernel	3.11.5
Python	3.11.5
Specific Python Package Versions used:	Matplotlib 3.7.2 Numpy 1.24.3 Pandas 2.0.3 Regex 2022.7.9 Scipy 1.11.1 Seaborn 0.12.2

3 KnowBe4

After designing and implementing the Phishing Simulation Tests according to the chosen specification, they were run in KnowBe4 over 3 days, and monitored over the next 4 weeks for recipients opening them and clicking the link inside or scanning the QR code. Once complete, the report section of KnowBe4 was used to generate a report including the performance of each user in each company. The chapters below specify how to set up a phishing campaign, and templates used.

3.1 Allow Phish Simulation Mails

Prior to rolling out the Setup for a phishing simulation test in KnowBe4 included creating and running an identical test campaign to ensure the email appears as expected, and ensuring that test emails aren’t blocked by email gateway defense systems.

The guide at https://support.knowbe4.com/hc/en-us/articles/203645138-Whitelisting-Guide was followed to ensure that the IP addresses that the emails originate from would be allowed. They were added to Microsoft Defender and Mimecast for Com1, and to Microsoft Defender for Com2. IP addresses and domains to be allowed in the advanced delivery policy at Microsoft Defender, and in MimeCast and other email systems are: 147.160.167.0/26, 52.49.201.246,

[2] Accessed at https://eu.knowbe4.com/ui/management/dashboard

52.49.235.189, 23.21.109.197, 23.21.109.212 and domains psm.knowbe4.com, *.telefon-de.com, *.kb4.io (further instructions at the link above).

3.2 Alert Tuning in Microsoft Defender

Since both Mimecast and Defender are protecting Com1 the emails were alerted as suspicious, but weren't blocked as the IP origination was allowed. However, this was tuned in the Alert tuner to avoid having new incidents created.

- Sign into Microsoft Defender and click "Settings" at the bottom left of the page.
- From the Settings page, click "Microsoft Defender XDR".
- Under Rules, click "Alert tuning" on the left pane.
- Click Add new rule to create the new rule based on the current campaign. A previous rule can also be modified from the previous campaign
- In the Tune alert page, click the service sources from the "Select service sources" dropdown and specify the conditions
- Set the condition as "Trigger > Equals > File" evidence type.
- Specify the email subject and the sender email address to only tune alerts for this campaign.
- Choose to resolve the alert as expected, categorise as information security, security training. Save the alert tuner with a specific name for this campaign.

3.3 New Phishing Campaign

Create a phishing campaign for phishing data. Log in with password to KnowBe4 mamagement console at https://eu.knowbe4.com/ui/management.

- Go to Accounts, click to enter the account for the new campaign.
- Choose the Phishing menu and Create New Campaign.
- Enter a campaign name.
- Choose One-Time as the frequency (doesn't need to be repeated).
- Enter a start date and time. Choose send emails over 3 business days. The emails are sent during the business hours set below in the same time zone set.
- Set track activity to one month or 4 weeks, to leave the failure checking page live for people on holidays, leave, etc. This is essential to ensuring that all clicks are counted, where possible.
- Track replies can be set to allow examination of out of office replies for information which shouldn't be included (Not set in this campaign).
- From Template Categories, choose the template to use. Ours is screenshot in Figure 1 in chapter 7, a modified version of an Amazon Prime day email. A modification of this one also included a QR code for Com2.
- Otherwise, difficulty ratings can be set to choose from a selection. If send localised emails is selected it will translate the email if a translation is available. We didn't use it as it would have introduced an extra confounder into the study.
- Phish Link Domain (domain appearing when hovering over a link in email) was set to eu-api.mimecast.com.kb4.io for Com1 (which normally has a different MimeCast link seen when hovering) and 2fa.telecom-de.com for Com2.

- The landing page was set to a company branded template: Classic SEI landing page with “Rules to Stay Safe Online”. This page is screenshot in Figure 4 and Figure 5 and advises the user of the phish and indicates in the email how they can tell it’s a phish.
- A group to add clickers to can be selected, for tracking and for assigning additional training, as required.
- Then Create Campaign can be clicked. The campaign will start sending out emails on the start date, and stop at the end date.

Activity on the campaign can be looked at from the opening date of the campaign, and a full report can be extracted once the campaign has closed after the tracking time. See Chapter 3.4 for details on exporting data.

3.4 Export Data for processing

Go to Reports, then Training -> All Training Activity -> Choose All Training Activity, All Accounts, All Users, Under campaign history, the chosen campaigns from 2023 and 2024 were selected, with Date range set from 2nd January 2023. In Additional filters, choose all user statuses, to be able to see data from users whose accounts have been duplicated. In the Add/Remove Columns section for output, ensure that only training status, enrolled on, completed on, time spent, along with the account and full name of the user in the general section. Save Report and click to generate a csv file, then download it either from the download centre in Reports, or the notification bar at the top left.
Then go to All Phishing Activity under the Reports menu. Choose all phishing activity, all accounts, all users, and the 2023 and 2024 official phishing campaign names under each company account. Date range is again from 2nd January 2023, and all user statuses and phishing outcomes. Set the columns to include the full user name again, and tick to include QR code scanned, IP address, browser and version, and Operating System. Again, save and generate a csv, then download it from the download centre in Reports, or the notification bar at the top left.
User reports need to generated under their accounts, so go to the Accounts menu and enter each account separately to run their reports: Users menu -> Status Active. Set the columns to include languages, email address and name information. Then generate csv.

4 Initial Processing and Anonymisation

Open the ids2.ipynb file import 4 CSV files from the same directory (2 user names files, one training activity, one phishing activity.

Expected filenames and column names are:

Table III: Expected filenames and columns for initial processing

Data	Filename	Column names required (Ignores others)
Training	all_training_activity.csv	Email, First Name, Last Name, Account, Campaign Name, Training Status, Enrolled On, Completed On, Time Spent

Phishing data	all_phishing_activity.csv	Email, First Name, Last Name, Campaign Name, Delivered, Opened, Clicked, Bounced, Browser, Operating System, IP Address, Account, IPLocation
Com1 user information	grp1 users active incl language.csv	Email, Name, First Name, Last Name, Risk Score, Groups, Archived At, Phishing Language, Training Language, Admin Language
Com2 user information	grp2 users active incl language.csv	Email, Name, First Name, Last Name, Risk Score, Groups, Archived At, Phishing Language, Training Language, Admin Language

Click Run All in the Cell menu to perform the cleaning. Ensure all tasks completed and open the output files (anon) for the cleaned and anonymised data.

Trainfile = 'Processed_Anon_Training_Data.csv'
Phishfile = 'Processed_Anon_Phishing_Data.csv'
User information with email addresses and names, in case of addition of new users Processed_User_Data.csv. This will not be used in the next step.
Anonymous info used = 'Processed_Anon_User_Data.csv'

5 Data Collation

11,060 users of the system were identified as active users and the above processed files can be opened and processed and collated further in processing3.ipynb. Open the file in Jupyter Notebook and click Run All in the Cell menu to perform the processing and analysis. Ensure all tasks completed. Results are in Resultsdf dataframe, where possible. Visualisations are output to the screen and files in the same directory locally.

This file collates all the anonymised training, phishing and collating data into a single file. Phishing and training data were reduced from 35,000 and 39,000 respective entries to 30,000 and 29,000.

Issues dealt with in this script are:
Duplicate users with complete and incomplete training. Several completed training courses to be combined in 2023 data.
Conversion of dates and times output by KnowBe4 into Epoch numbers for time calculations.
Conversion of training durations to minutes, addition of multiple completed training entries for some years.
Calculating days since training completed, dealing with days since training completed when training may have been completed for Q3, but not Q2.

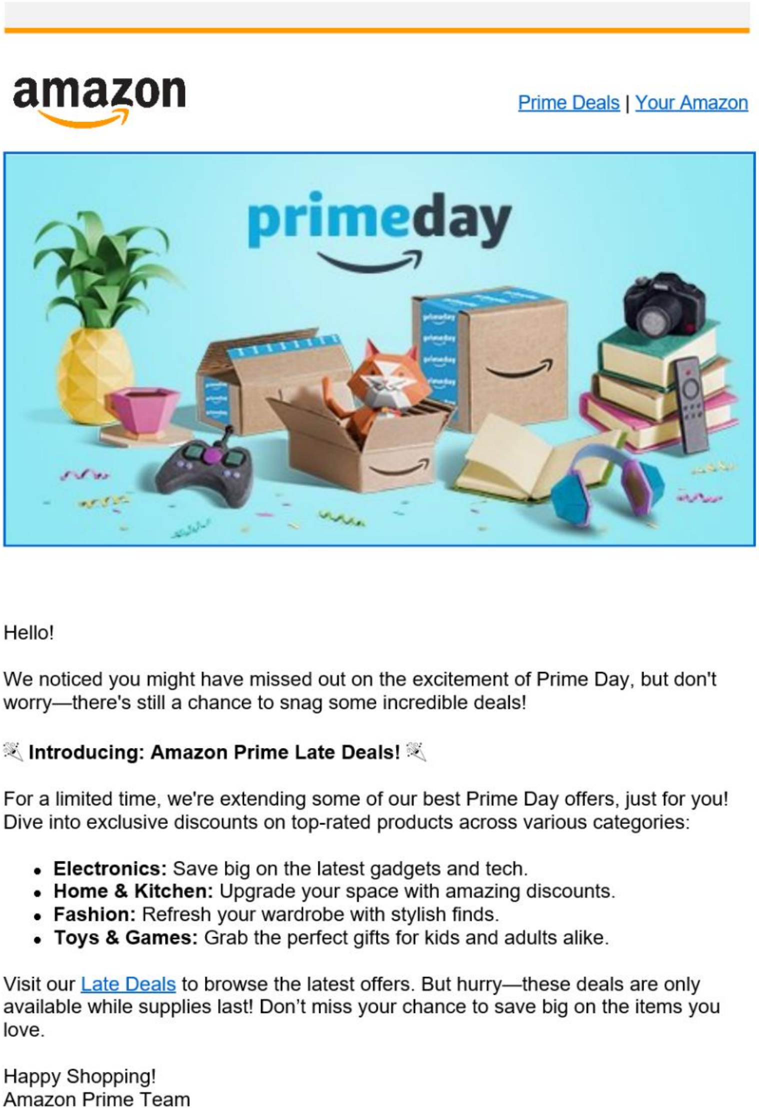
Combining the 3 dataframes into one.

6 Analysis

Calculating results between the different tests.
Calculating statistics including mean, mode, median, etc.
Look for dependence with Pearson correlation, Chi squared for categorical data.
Creating pair plots to visualise any linear or non-linear relationships.
Creating pie charts and histograms, and bar charts for visualisation of data.

The results output and correlations and statistics performed then need to be reviewed for interpretation.

7 Phishing Templates



Hello!

We noticed you might have missed out on the excitement of Prime Day, but don't worry—there's still a chance to snag some incredible deals!

🎉 **Introducing: Amazon Prime Late Deals!** 🎉

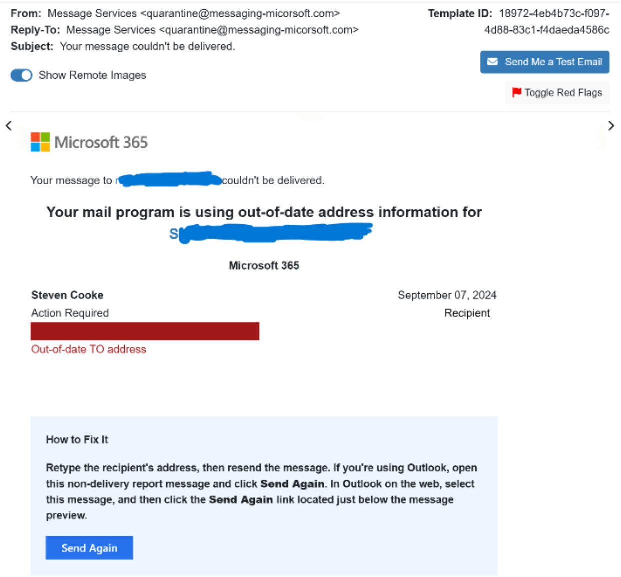
For a limited time, we're extending some of our best Prime Day offers, just for you! Dive into exclusive discounts on top-rated products across various categories:

- **Electronics:** Save big on the latest gadgets and tech.
- **Home & Kitchen:** Upgrade your space with amazing discounts.
- **Fashion:** Refresh your wardrobe with stylish finds.
- **Toys & Games:** Grab the perfect gifts for kids and adults alike.

Visit our Late Deals to browse the latest offers. But hurry—these deals are only available while supplies last! Don't miss your chance to save big on the items you love.

Happy Shopping!
Amazon Prime Team

Figure 1: Q3 2024 Phishing Email (modified template from KnowBe4)



From: Message Services <quarantine@messaging-micorsoft.com>
Reply-To: Message Services <quarantine@messaging-micorsoft.com>
Subject: Your message couldn't be delivered.

Template ID: 18972-4eb4b73c-f097-4d88-83c1-f4daeda4586c

Your message to [redacted] couldn't be delivered.

Your mail program is using out-of-date address information for
[redacted]

Microsoft 365

Steven Cooke
Action Required

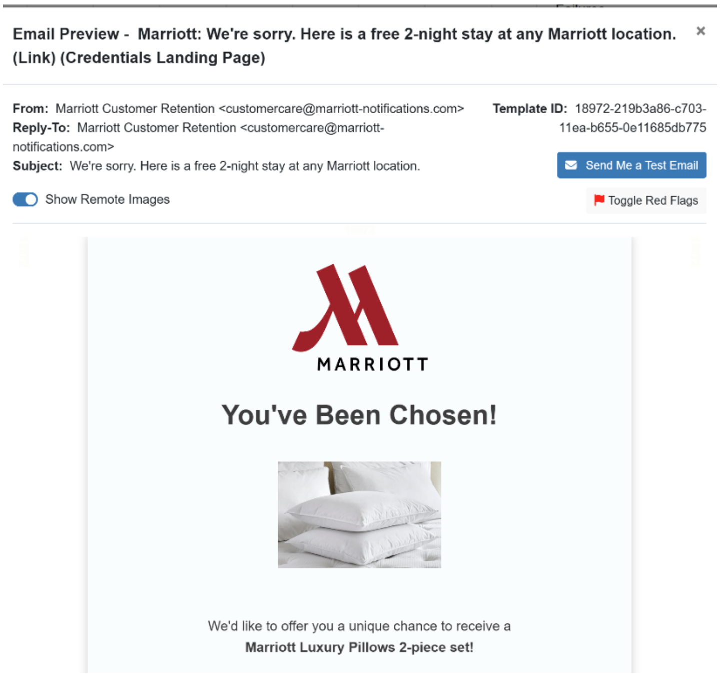
September 07, 2024
Recipient

Out-of-date TO address

How to Fix It

Retype the recipient's address, then resend the message. If you're using Outlook, open this non-delivery report message and click **Send Again**. In Outlook on the web, select this message, and then click the **Send Again** link located just below the message preview.

Figure 2: 2023 Phishing Email Template (email address redacted)



Email Preview - Marriott: We're sorry. Here is a free 2-night stay at any Marriott location. (Link) (Credentials Landing Page) ×

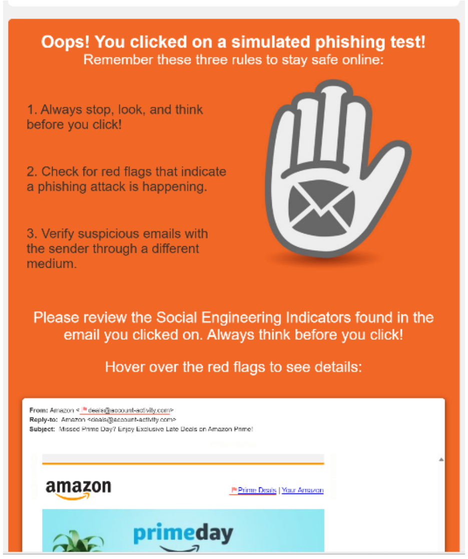
From: Marriott Customer Retention <customercare@marriott-notifications.com>
Reply-To: Marriott Customer Retention <customercare@marriott-notifications.com>
Subject: We're sorry. Here is a free 2-night stay at any Marriott location.

Template ID: 18972-219b3a86-c703-11ea-b655-0e11685db775

You've Been Chosen!

We'd like to offer you a unique chance to receive a **Marriott Luxury Pillows 2-piece set!**

Figure 3: 2024 Q2 Phishing Email Template



Oops! You clicked on a simulated phishing test!
Remember these three rules to stay safe online:

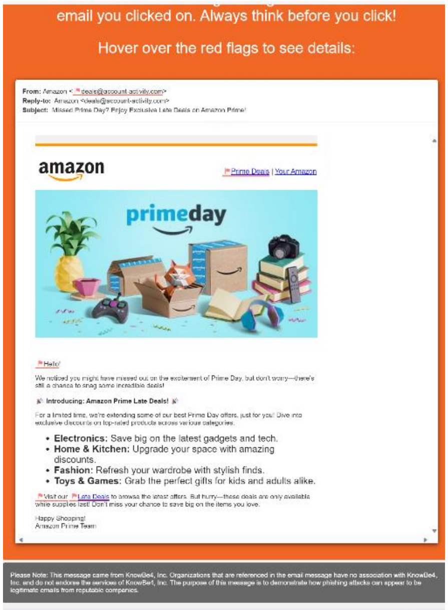
1. Always stop, look, and think before you click!
2. Check for red flags that indicate a phishing attack is happening.
3. Verify suspicious emails with the sender through a different medium.

Please review the Social Engineering Indicators found in the email you clicked on. Always think before you click!

Hover over the red flags to see details:

From: Amazon <deals@account-activity.com>
Reply-to: Amazon <deals@account-activity.com>
Subject: Missed Prime Day? Enjoy Exclusive Late Deals on Amazon Prime!

Figure 4: 2024 Landing Page seen after clicking



email you clicked on. Always think before you click!

Hover over the red flags to see details:

From: Amazon <deals@account-activity.com>
Reply-to: Amazon <deals@account-activity.com>
Subject: Missed Prime Day? Enjoy Exclusive Late Deals on Amazon Prime!

Hello!

We noticed you might have missed out on the excitement of Prime Day, but don't worry—there's still a chance to snag some incredible deals!

Introducing: Amazon Prime Late Deals!

For a limited time, we're extending some of our best Prime Day offers, just for you! Dive into exclusive discounts on top-rated products across various categories.

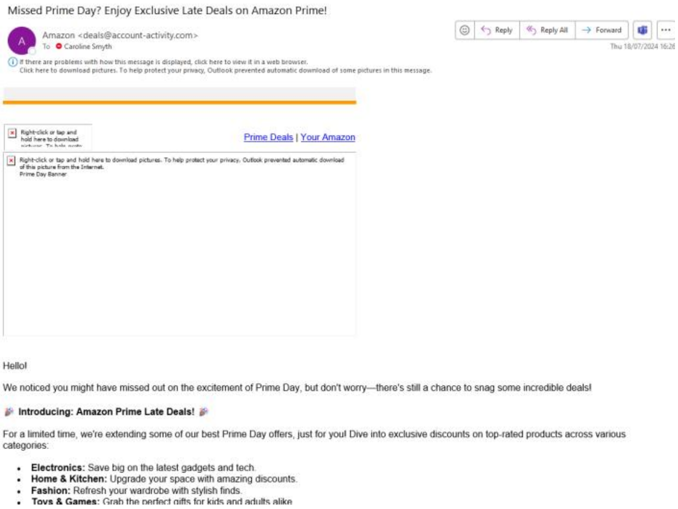
- **Electronics:** Save big on the latest gadgets and tech.
- **Home & Kitchen:** Upgrade your space with amazing discounts.
- **Fashion:** Refresh your wardrobe with stylish finds.
- **Toys & Games:** Grab the perfect gifts for kids and adults alike.

Visit our Late Deals to browse the latest offers. But hurry—these deals are only available while supplies last! Don't miss your chance to save big on the items you love.

Happy Shopping!
Amazon Prime Team

Please Note: This message came from KnowBe4, Inc. Organizations that are referenced in the email message have no association with KnowBe4, Inc. and do not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can appear to be legitimate emails from reputable companies.

Figure 5: Bottom of landing page, red flags indicate items which are suspicious and explains why



Missed Prime Day? Enjoy Exclusive Late Deals on Amazon Prime!

Amazon <deals@account-activity.com>
To Caroline Smyth

Thu 18/07/2024 16:28

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Right-click or tap and hold here to download pictures. To help protect

Prime Deals | Your Amazon

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Prime Day Banner

Hello!

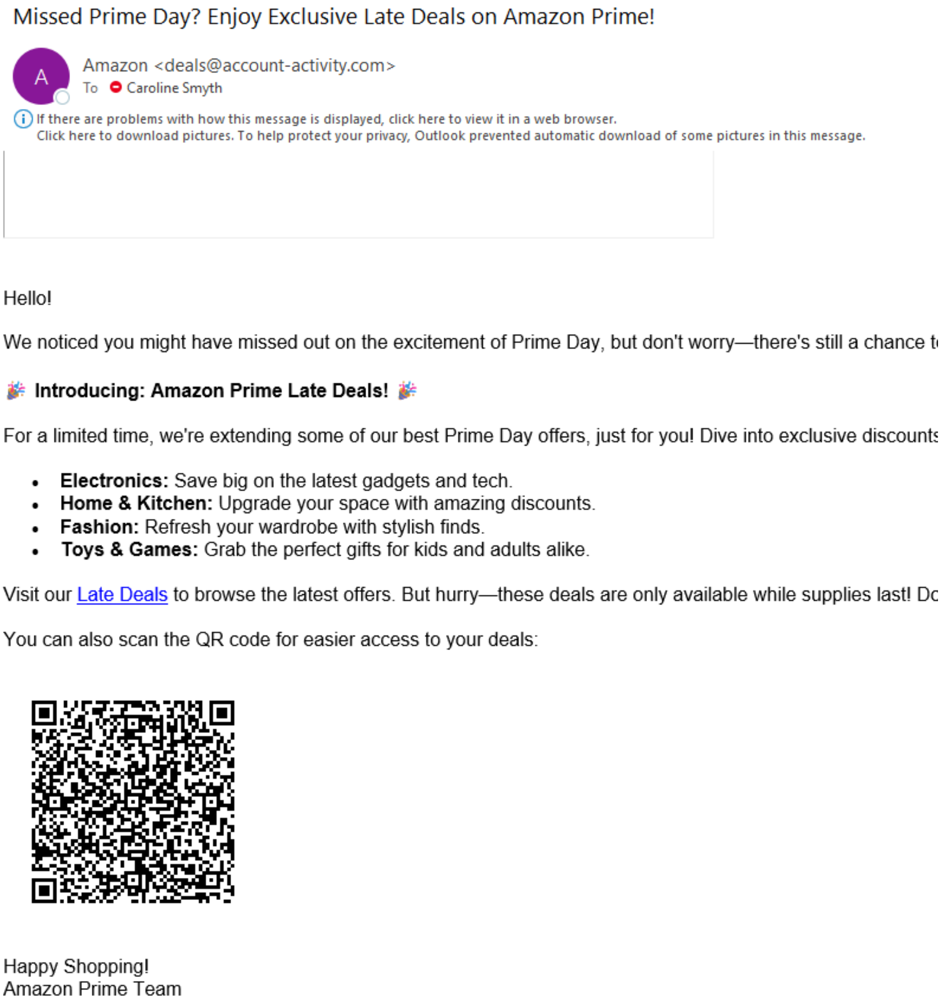
We noticed you might have missed out on the excitement of Prime Day, but don't worry—there's still a chance to snag some incredible deals!

Introducing: Amazon Prime Late Deals!

For a limited time, we're extending some of our best Prime Day offers, just for you! Dive into exclusive discounts on top-rated products across various categories:

- **Electronics:** Save big on the latest gadgets and tech.
- **Home & Kitchen:** Upgrade your space with amazing discounts.
- **Fashion:** Refresh your wardrobe with stylish finds.
- **Toys & Games:** Grab the perfect gifts for kids and adults alike

Figure 6: Shows how the email will appear in most users' email inbox, unless they've set to download pictures automatically



Missed Prime Day? Enjoy Exclusive Late Deals on Amazon Prime!

Amazon <deals@account-activity.com>
To Caroline Smyth

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hello!

We noticed you might have missed out on the excitement of Prime Day, but don't worry—there's still a chance t

🎉 **Introducing: Amazon Prime Late Deals!** 🎉

For a limited time, we're extending some of our best Prime Day offers, just for you! Dive into exclusive discounts

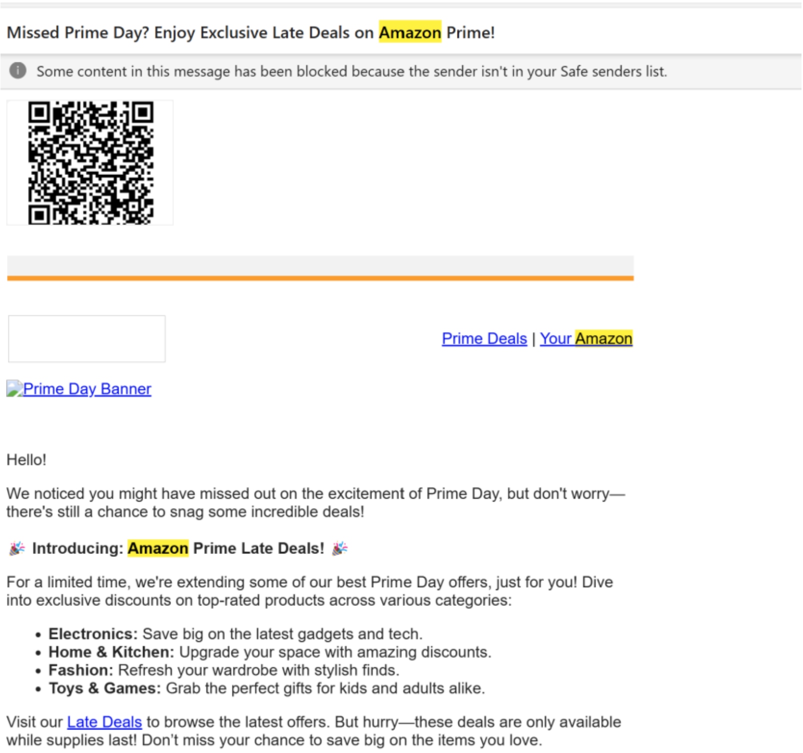
- **Electronics:** Save big on the latest gadgets and tech.
- **Home & Kitchen:** Upgrade your space with amazing discounts.
- **Fashion:** Refresh your wardrobe with stylish finds.
- **Toys & Games:** Grab the perfect gifts for kids and adults alike.

Visit our Late Deals to browse the latest offers. But hurry—these deals are only available while supplies last! Dc

You can also scan the QR code for easier access to your deals:

Happy Shopping!
Amazon Prime Team

Figure 7: Modification of the email showing a QR code embedded, used in Com2 campaign



Missed Prime Day? Enjoy Exclusive Late Deals on Amazon Prime!

Some content in this message has been blocked because the sender isn't in your Safe senders list.

Prime Deals | Your Amazon

Prime Day Banner

Hello!

We noticed you might have missed out on the excitement of Prime Day, but don't worry—there's still a chance to snag some incredible deals!

🎉 **Introducing: Amazon Prime Late Deals!** 🎉

For a limited time, we're extending some of our best Prime Day offers, just for you! Dive into exclusive discounts on top-rated products across various categories:

- **Electronics:** Save big on the latest gadgets and tech.
- **Home & Kitchen:** Upgrade your space with amazing discounts.
- **Fashion:** Refresh your wardrobe with stylish finds.
- **Toys & Games:** Grab the perfect gifts for kids and adults alike.

Visit our Late Deals to browse the latest offers. But hurry—these deals are only available while supplies last! Don't miss your chance to save big on the items you love.

Figure 8: How the email appears in the inbox. The QR code is at the top of the mail