

# The Phishermen: User Study Protocol

Hila Lewin  
Abdullah Garra  
Lilach Daniel

## 1 APPENDIX A: PROTOCOL

Today, we will introduce a phishing detection Chrome extension that we developed and later gather your feedback about it. We want to emphasize that this is not a test of your knowledge. We are trying to thoroughly examine our extension. The study will be conducted in two stages. In Stage 1, we will divide participants into two main groups. The first group will have the extension installed on their computers and will be further divided into sub-groups, while the second group will not have the extension, nor it will be divided into sub-groups. We will request permission from both groups to monitor their email behaviors throughout the experiment, we will only record your behaviors only in the context of the emails we send you. This stage will span over three months. In stage 2, we'll gather all participants to collect feedback with regards to our chrome extension's usability through a survey. We remind you that when registering for the study you were asked to answer some questions about your background:

- (1) What is your profession?
- (2) What is your age?
- (3) How frequently do you use your Gmail account? (Rate 1-5)
- (4) Do you have any prior knowledge of cybersecurity? (Rate 1-5)
- (5) Are you familiar with the concept of phishing? If so, can you explain what phishing means to you?
- (6) Do you understand the risks associated with phishing? (Rate 1-5)
- (7) Have you ever been a victim of a phishing attack? Yes/No  
If yes, please provide details.
- (8) Do you currently use any tools to protect yourself from phishing? Yes/No
- (9) How often do you encounter phishing attempts in your daily email activity? (Rate 1-5)

Your answers were analyzed in a way that defines a fair group division.

### 1.1 Stage 1: Extension Usage

After dividing participants into groups, we will proceed to install the extension on part of your computers, depending on the group you're in. The extension's primary function is to notify you when it detects various types of phishing traits, according to the configurations you have on your browser. Feel free to ask any questions regarding the extension's functionality. In addition to your usual email activity, during the study period, you will receive a series of emails. Some of these emails will be legitimate, while others will be simulated phishing emails. (Email examples can be found in appendix B.) Each participant will be part of a specific group within this study, which will influence how the extension functions for him/her. Some participants will have the freedom to customize their extension's settings, while others will be assigned specific predefined settings.

All participants will receive the same set of emails throughout the study regardless of the group they belong to.

**1.1.1 Group Assignment.** We will now assign each participant to a group. The group with the extension installed will be further divided into sub-groups with one having the freedom to customize the extension and the other sub-groups will have a predefined configuration of the extension. (Sub-group division suggestion can be found in appendix C)

**1.1.2 Extension installation.** Participants in the group without the extension are free to go.

We will now share a link to our extension in the Chrome Web Store with you. Please add the extension to your browser. If you find any trouble working with the Chrome Web Store, feel free to reach out to us for assistance. You are welcomed to activate the extension on your browser with your Gmail account.

Those with the predefined configurations are asked to set the configurations with respect to the group they belong to. If you have any questions about customizing the extension, please feel free to ask us. Meanwhile, we will ensure that each fixed-configuration sub-group has the correct settings in place. Please do not change these configurations throughout the study period. Now that you have the extension, you are asked to answer the following question which will serve us in stage 2.

- How hard was it to activate the extension on your browser? (Rate 1-5)

Only those who have a predefined configuration are asked to answer the following question:

- How challenging was it to configure the extension with the settings we assigned to you?

Thank you for taking part in our study. Everyone is free to go now, Happy anti-phishing.

### 1.2 Stage 2: Survey on Extension Usability

Today, we've gathered you here three months after providing you with our phishing detector to evaluate its usability. Your feedback is crucial in helping us understand how user-friendly our extension is. We will evaluate the usability of our extension through a survey, which we will present to you shortly. Please feel free to ask for clarification if any questions are unclear. The survey:

- a) **Comprehensibility:**
  - How difficult was it to understand the feature explanations? (Rate 1-5)
  - How challenging was it to comprehend the security and privacy advice presented by the extension? (Rate 1 - 5)
- b) **Actionability:**

- How time-consuming was it to read and understand the explanation associated with each feature? (Rate 1 - 5)
  - How time-consuming was it to read and understand the advice provided by the extension? (Rate 1 - 5)
  - For each feature, did you think the sub-features (High/Low or extended/simple) was helpful? (Rate 1-5 for each feature that has sub-features independently). Please explain.
  - To what extent do you think the content feature should have sub-features? (Rate 1-5)
    - In case you think it needs to have sub-features, you are welcomed to make suggestion.
  - What did you like/dislike about each feature? (consider: (1) response time, (2) perceived security performance)
  - Only participants with predefined configurations are asked to answer the following questions:
    - How much would you have preferred to change the configurations you had throughout the study? (Rate 1-5)
    - How much would you have preferred the freedom to customize the settings? (Rate 1-5)
    - Did the configuration suit your needs and routine?
  - Only participants with customized configurations are asked to answer the following questions:
    - Which configuration suited your needs and routine best?
    - How much would you have preferred a predefined configuration? (Rate 1-5)
  - **Disruptiveness:**
    - How much did the notification frequency disturb you? (Rate 1-5)
    - To what extent did the extension's recommended behaviors disrupt your existing habits or routines? (Rate 1-5)
    - How acceptable were the extension's popups frequency in exchange for enhanced security? (Rate 1-5)
    - How much did the notification frequency disrupt your daily activity? (Rate 1-5 for each feature you used) please explain.
    - To what extent did the runtime disrupt your daily activity? (Rate 1-5 for each feature you used) please explain.
- c) **Compliance:**
- For each feature, how well did you comply with its notifications? (Rate 1-5 or choose 'did not have' or 'did not use' if you didn't use or have the feature.)
    - If you haven't followed some of the advice, please give some details.
- c) **General Questions:**
- Did the extension have the right number of features? (Rate 1-5)

- Should we consider (Adding/removing) features? In case you think the number of features was not suitable please explain.

- Considering your experience, how likely are you to continue using our extension? (Rate 1-5)
- Only participants with predefined configurations are asked to answer the following question:
  - Considering your experience, how likely are you to continue using our extension with the \*provided configuration\*? (Rate 1-5)

## 2 APPENDIX B: EMAIL EXAMPLES AND THE CORRESPONDING WARNINGS

### 2.1 [Content, Links, Urgency]

"Dear User,

We apologize for the inconvenience but we have detected an unusual activity in your account.

Our system have noticed that someone else tried to access your account from an unrecognized location. We take your account security seriously and that's why we're reaching out to you for immediate assistance.

Please, click on the link below to verify your identity and secure your account. If you don't take action within the next 24 hours, your account might be suspended indefinitely! <https://secure000-webpaypal.com/signin/>

Don't wait until it's too late! Act NOW to prevent unauthorized access and potential loss of sensitive information.

We appreciate your prompt attention to this matter. If you encounter any difficulties or have questions, contact our support team at [help@secure000-webpaypal.com](mailto:help@secure000-webpaypal.com) Remember, your security is our top priority!

Best Regards, Ash Account Security Department"

### 2.2 [Content, Urgency]

"Dear Stream User,

We are writing to inform you about an urgent update required for our app. Your current version is outdated and could potentially lead to security vulnerabilities and data integrity issues. To ensure the seamless and secure operation of our app, we have attached the latest update file to this email. Please download the attached file and follow the installation instructions provided below:

- 1) Download the attached file: "AppUpdate.zip"
- 2) Extract the contents of the ZIP file to a location on your device.
- 3) Locate and run the "UpdateInstaller.exe" file.

It is crucial to perform this update immediately to prevent any disruptions in your app experience and to maintain the security of your data. We apologize for any inconvenience this may cause and appreciate your prompt action.

Please let us know if you encounter any difficulties during the update process by contacting our support team.

Best regards,  
Lilach"

## 2.3 [Content, Grammar]

"Dear Giroud,

We trust your having a productive coding experience with our integrate development environment (IDE). We're excited to inform you about the latest update that's available for download, design to enhance your coding workflow and provide you with new features and optimizations.

Important Note: Before proceeding with the update, please insure you back up your current projects and settings to avoid any potential data loss.

Attached to this email, you'll find the installer file for the updated version off our IDE. This update includes:

- 1) Improved code suggestions and auto-completion.
- 2) Enhanced debuggin tools for better error identification.
- 3) Compatibility with the latest programming languages and libraries.
- 4) Streamlined user interface for a more intuitive experience.

To updates your IDE, please follow this steps:

Download the attached file: "VS\_Update\_2023.exe"

Run the installer and follow the on-screen instructions.

Once the update is complete, launch the IDE and enjoy the new features!

Should you encounters any issues during the update process or have questions about the new features, our support team are ready to assist. Reach out to us at support@gatcoins.io.com for prompt assistance.

We values you're commitment to using our IDE and hopes this update elevates you're coding journey. Thank you for choosing VSCODE for you're development needs.

Happy coding!

Best regards, VScode"

## 2.4 [Urgency]

"Hi Alex,

I've had a chance to review the submission you shared. It looks promising, and I believe it's important for us to sit down and discuss it further as soon as possible.

Could we arrange a meeting at your earliest convenience to go over the details and address any questions or points that may arise from the submission? Your insights are valuable, and I'm looking forward to collaborating with you to move this forward effectively."

## 2.5 []

"Dear Shila,

I hope this email finds you well and in good spirits. It's been far too long since we last caught up, and I've been thinking about all the fun times we've had together and the memories we've created. Life has been quite a rollercoaster lately, and I thought it would be wonderful to reconnect and share what's been going on.

First and foremost, I want to hear all about what's new in your life. How are you and your family? Have you taken any exciting trips or started any interesting projects? Please fill me in on all the details—I'm eager to catch up. As for me, I've had my fair share of ups and downs, but I've been keeping busy. I started a new job last year, and it's been both challenging and rewarding. The learning curve has been steep, but I'm surrounded by great colleagues who

have been incredibly supportive.

Call me up when you are free :)"

## 2.6 [Urgency-high]

"Hi Adam,

I wanted to let you know that I've viewed the submission you shared. It looks promising, and I believe it's important for us to sit down and discuss it further as soon as possible.

Could we arrange a meeting when you are free, to go over the details and address any questions or points that may arise from the submission?"

## 2.7 [Content, First Time Domain]

"Dear Daniel,

We are excited to inform you about the opportunity to apply for a Visa credit card with exclusive benefits and privileges. This is a limited-time offer that you wouldn't want to miss out on.

Our Visa credit card offers:

1. Low interest rates
2. Generous credit limits
3. Cashback rewards on every purchase
4. Access to a wide network of ATMs worldwide

To take advantage of this special offer, all you need to do is reply to this email with your interest. Our dedicated team will guide you through the quick and hassle-free application process.

Please provide us with the following information in your reply:

1. Full Name
2. Contact Number
3. Mailing Address

Our team is ready to assist you with any questions you might have about the application process or the benefits of our Visa credit card. Don't miss this opportunity to enhance your financial freedom and enjoy the convenience of a Visa credit card. Simply reply to this email, and we will take care of the rest.

We look forward to serving you and helping you make the most of this exclusive offer.

Best regards, Paypal"

## 2.8 [Content, Urgency-high]

"Hey Ronald,

We've noticed that you're having trouble registering to the website. I believe that it's important to have your account created and see how we can work this out when you are available.

Please reply to this email as soon as you are available.

We hope you could provide us with your phone number, visa number and the verification code you will get once we reply to you."

## 3 APPENDIX C: SUB-GROUP DIVISION SUGGESTION

Considering all possible sub-groups would necessitate a significant number of participants, making it impractical to conduct a pilot study. Therefore, we aim to create sub-groups that achieve pairwise coverage of all features options. Given our extension's design (figure 1), the number of options for each feature will determine the number of different values for that feature: Content values will be {0,1}, Link

detection values will be {0, 1, 2}, Urgency detection values will be {0, 1, 2}, Grammar detection values will be {0, 1, 2}.

**Custom Preferences Selection  
for all sessions**

? ☒ Phishing Content Detection  
 ? ☒ Phishing Links Detection  
 ? ☒ Bad Grammar/Spelling Detection  
 ? ☒ Urgency Detection

Sensitivity: Low High

Sensitivity: Low High

Save and Close

**Figure 1: User Preferences UI**

We used a tool (<https://pairwise.teremokgames.com/3x2e8/>) to generate a pairwise coverage of these values. The tool considered the 0,0,0,0 configuration which we replaced manually. Each configuration is associated with a sub-group resulting in 10 sub-groups overall.

Content	Link	Urgency	Grammar
0	1	1	1
1	1	2	0
1	2	0	1
1	0	1	2
0	2	1	0
0	0	2	1
0	1	0	2
1	0	0	0
0	2	2	2

**Table 1: Sample Data**