PhishGuard — Easy Step-by-Step Guide

Follow these simple instructions to start the PhishGuard helper and load the browser extension. After testing each website, complete the short feedback survey at the end of this document.

Before You Start

- Make sure you have downloaded and unzipped the test package to a place you can find (for example, your Desktop).
- Keep the computer connected to the internet for the duration of the test.
- If any step fails, note the step name and contact the study coordinator.

How to Extract (Unzip) the Test Package

Windows

1. Locate the downloaded ZIP file (e.g., `PhishGuard_Test_Package.zip`) — likely in your **Downloads** folder.
2. Right-click the ZIP file and choose **Extract All...**.
3. In the dialog, choose a destination folder (suggestion: **Desktop**) and click **Extract**.
4. A new folder will appear containing `1_Load_Extension`, `2_Run_Me_Backend`, `test_websites_list.html`, and the instructions PDF.

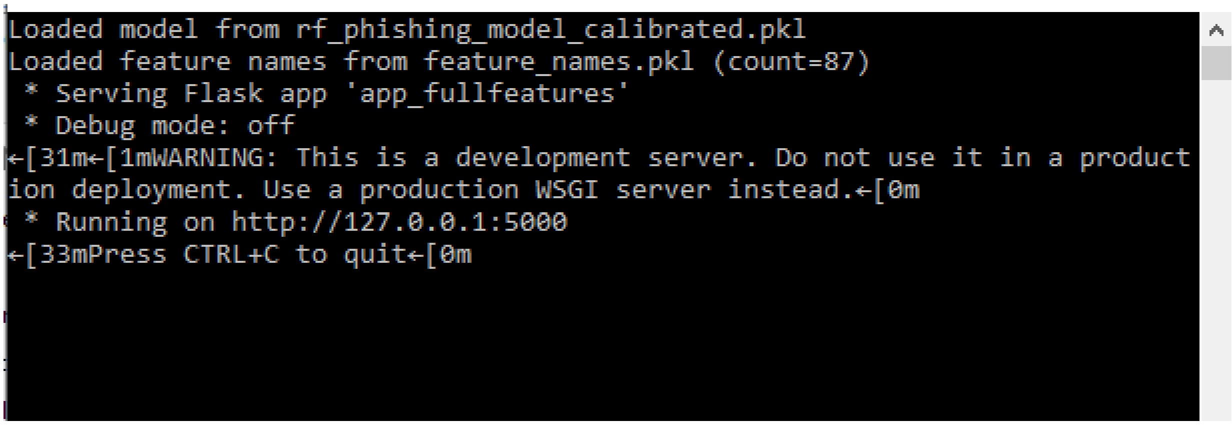
macOS

1. Double-click the ZIP file.
2. The archive will be decompressed automatically and a folder will appear in the same location.
3. Open that folder to see `1_Load_Extension`, `2_Run_Me_Backend`, `test_websites_list.html`, and the instructions PDF.

Step 1 — Start the PhishGuard Helper (Backend)

1. Open the folder named **2_Run_Me_Backend**.
2. Double-click **Start_Phishing_Detector.exe** (Windows) or the provided launcher for mac (if included).

3. A small terminal window will open and display:
   Running on http://127.0.0.1:5000
   Leave this window open while you test. This means the helper is active and ready to respond to the extension.



```
Loaded model from rf_phishing_model_calibrated.pkl
Loaded feature names from feature_names.pkl (count=87)
 * Serving Flask app 'app_fullfeatures'
 * Debug mode: off
←[31m←[1mWARNING: This is a development server. Do not use it in a product
ion deployment. Use a production WSGI server instead.←[0m
 * Running on http://127.0.0.1:5000
←[33mPress CTRL+C to quit←[0m
```

If you see an error when opening the file, note the error text and contact the researcher.

Step 2 — Load the Chrome Extension (Developer Mode)

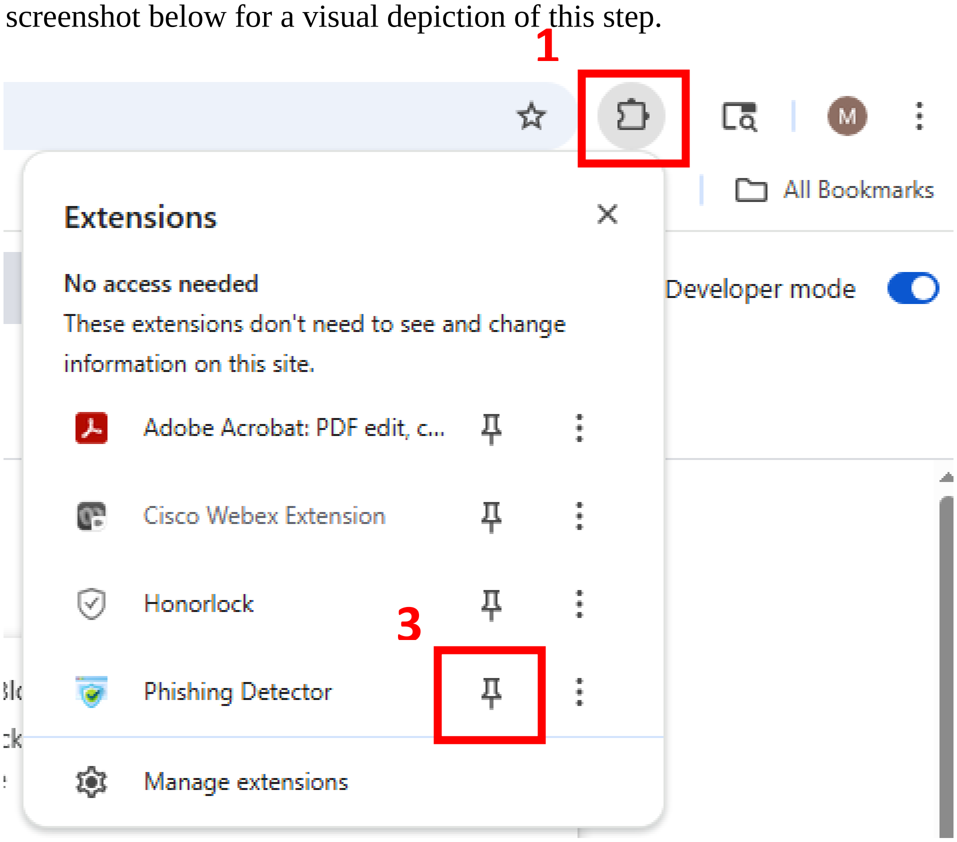
You only need to load the extension once per session. Keep the helper window open while testing.

1. Open **Google Chrome**.
2. In the address bar, type `chrome://extensions` and press **Enter**.
3. Turn on **Developer mode** (toggle in the top-right corner).
4. Click **Load unpacked** (top-left button).
5. In the file dialog, select the folder named **1_Load_Extension** and click **Select Folder** (or **Open**). Do not double click into the **1_Load_Extension** folder; simply single click it to select it, and then click **Select Folder** on the bottom right of the screen.
6. The extension will appear on the extensions page with its name (e.g., *PhishGuard*).

Step 3 — Find & Pin the PhishGuard Icon in Chrome (so it's easy to access)

After loading the extension you may not see the icon directly in the toolbar. Pinning it makes it visible and easy to click.

1. Look for the **puzzle-piece icon** (Extensions) in the Chrome toolbar (near the top-right). Click it.
2. A dropdown list of installed extensions will appear. Find **PhishGuard** in the list.
3. Click the **pin icon** next to PhishGuard.
    - When the pin is solid/blue, PhishGuard is pinned and its icon will appear in the toolbar.
4. If you want the icon to remain in place, you can click and drag the icon to rearrange it in the toolbar.
5. See screenshot below for a visual depiction of this step.



Extensions

No access needed

These extensions don't need to see and change information on this site.

If the icon does not respond:

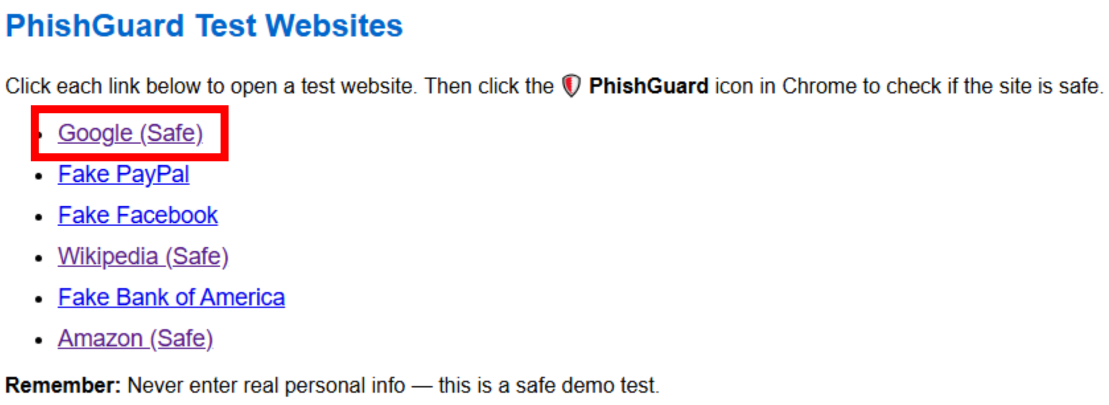
- Make sure the backend window says `Running on http://127.0.0.1:5000`.
- If not, double-click the `Start_Phishing_Detector.exe` again and wait for the "Running…" message.

Important Safety Note Before Proceeding

Do **not** enter any personal information, passwords, or payment details on any test websites. These sites are only for demonstration and testing.

Step 4 — Test the Websites

1. Open the file `test_websites_list.html` (double click it) and click the first link to open a test site in a new tab.



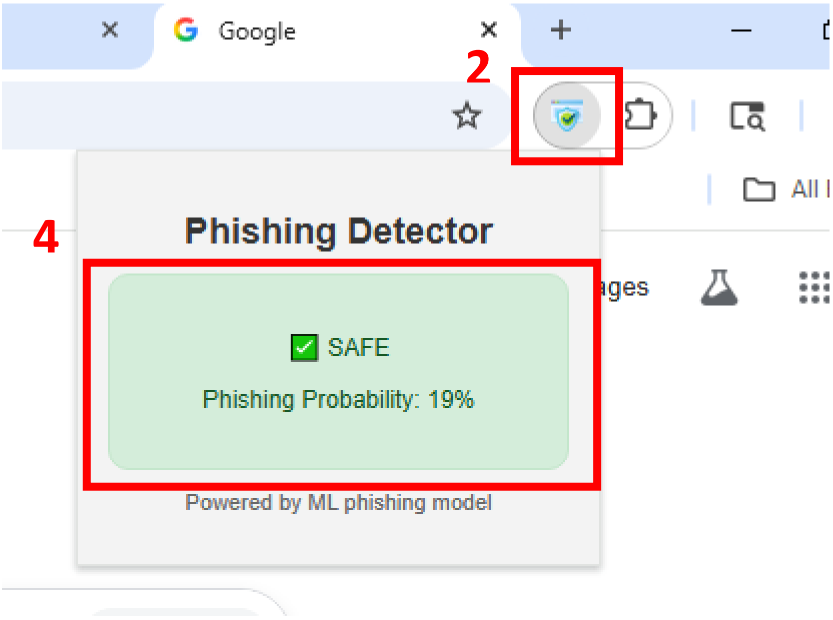
PhishGuard Test Websites

Click each link below to open a test website. Then click the 🛡 **PhishGuard** icon in Chrome to check if the site is safe.

- Google (Safe)
- Fake PayPal
- Fake Facebook
- Wikipedia (Safe)
- Fake Bank of America
- Amazon (Safe)

Remember: Never enter real personal info — this is a safe demo test.

2. After the page fully loads, click the **PhishGuard** icon in the Chrome toolbar.
3. Wait for the extension to analyze the site.
4. Note the result shown (e.g., **Safe**, **Suspicious**, **Unsafe**) and then move to the next site.
5. See screenshot below for visual depiction of this step.



Phishing Detector

✅ SAFE

Phishing Probability: 19%

Powered by ML phishing model

Suggested Test Sites (examples)

- Google — `http://www.google.com` (Expected: Safe)
- Wikipedia — `http://www.wikipedia.org` (Expected: Safe)
- Amazon — `http://www.amazon.com` (Expected: Safe)
- Fake PayPal — `http://secure-paypal.com.account.recovery.ru` (Expected: Unsafe)
- Fake Facebook — `http://update-facebook-login.tk` (Expected: Unsafe)
- Fake Bank — `http://bankofamerica.secure-login.xyz` (Expected: Unsafe)

Feedback Survey

After testing the list of websites, please complete the table below and the short questions.

Website Evaluation Table

Website (copy the full URL)	**PhishGuard result (Safe / Unsafe / Uncertain)**	**Did you agree with the result? (Yes / No)**	**Notes (optional)**
Google — http://www.google.com	SAFE 19%, SAFE 19%, SAFE 19%, SAFE 19%, SAFE 19%,	Yes, Yes, Yes, Yes, Yes	Confused why “SAFE” has a probability of 19%
Wikipedia — http://www.wikipedia.org	SAFE 36%, SAFE 36%, SAFE 36%, SAFE 36%, SAFE 36%,	Yes, Yes, Yes, Yes, Yes	Unsure why ‘SAFE’ has 36% probability.
Amazon — http://www.amazon.com	SAFE 19%, SAFE 19%, SAFE 19%, SAFE 19%, SAFE 19%,	Yes, Yes, Yes, Yes, Yes	
Fake PayPal — http://secure-paypal.com.account.recovery.ru	PHISHING 89%, PHISHING 89%, PHISHING 89%, PHISHING 89%, PHISHING 89%,	Yes, Yes, Yes, Yes, Yes	Recommend using “UNSAFE” instead of “PHISHING”
Fake Facebook — http://update-facebook-login.tk	SUSPICIOUS 79%, SUSPICIOUS 79%, SUSPICIOUS 79%, SUSPICIOUS 79%, SUSPICIOUS 79%,	Yes, Yes, Yes, Yes, Yes	

Website (copy the full URL)	**PhishGuard result (Safe / Unsafe / Uncertain)**	**Did you agree with the result? (Yes / No)**	**Notes (optional)**
Fake Bank — http://bankofamerica.secure-login.xyz	PHISHING 84%, PHISHING 89%, PHISHING 91%, PHISHING 84%, PHISHING 84%,	Yes, Yes, Yes, Yes, Yes	

Overall Questions (circle one)

1. How easy was it to follow the setup instructions?
   1 = Very Difficult 2 = Difficult 3 = Neutral 4 = Easy 5 = Very Easy
   Responses: 4, 3, 2, 1, 1

2. How clear were the extension's warnings?
   1 = Not Clear 2 = Somewhat Clear 3 = Neutral 4 = Clear 5 = Very Clear

Responses: 4, 5, 4, 5, 5

3. How much do you trust the extension's advice?
   1 = Not at All 2 = Slightly 3 = Neutral 4 = Mostly 5 = Completely

Responses: 5, 5, 4, 4, 4

4. How likely are you to follow the extension's recommendation in real life?
   1 = Not Likely 2 = Slightly Likely 3 = Neutral 4 = Likely 5 = Very Likely

Responses: 5, 4, 4, 4, 3

Optional Comments

Please describe any problems, suggestions, or comments about the setup or the extension behavior:

Recommend having extension automatically analyze upon entering each website.

Thank you for your participation. If you have questions, contact Michael Koppel at: mkoppel6@gatech.edu