Evaluating the Efficiency of Password Managers Against Real-World Phishing Pages

Mulla Mohsin Azimmohammed[1], Huzaif Shaikh Ismail Sofisarmast[2]
([1]MCA department, Sinhgad Institute of Business Administration and Research (SIBAR) , Pune, India
[2]MCA department, Sinhgad Institute of Business Administration and Research (SIBAR) , Pune, India
Email: [1]mullamohsin48@gmail.com, [2]hsofi261@gmail.com)

Abstract:

This study checks how password managers behave when visiting on realistic phishing pages. Testing was done in a virtual machine using Caniphish templates and XAMPP with host file trick. both browser managers including Chrome, Brave, Edge and Firefox and Standalone password managers including Bitwarden, Lastpass, Keepassxc, Proton Pass were manually tested. Findings indicate that the majority of password managers detected domain inconsistencies and prevented automatic credential filling, while certain cases necessitated manual input, and several browsers restricted access to websites because of certificate validation issues. This shows managers give safety in many cases but not always the same way. This research helps users know the limits of password managers. And also help the password manager developers make better systems.

Keywords — **password managers, phishing, autofill, browser security, authentication, cybersecurity.**

I. INTRODUCTION

In today's digital world almost every person depends on many online accounts. To handle these accounts password managers are used because they generate strong passwords save them and also autofill whenever required. These tools make things easy but at the same time attackers are also becoming smarter. Phishing is most used trick by the hackers or scammers used to scam other people in entering their credentials like passwords and usernames on realistic phishing sites. Phishing websites look same like real ones and many users enter details without knowing. Password managers are expected to stop autofill on fake sites but studies show they don't always behave the same. Some still autofill on phishing pages. So it becomes important to test them properly. This research will test different password managers on phishing pages to see how they react whether they autofill block or warn the user.

A. Statement of the Problem

Phishing attacks are increasing daily and millions of users are at risk of losing accounts and money
Password managers say they give safety against phishing but real protection is not always clear
Some managers protect strongly some may fail in certain conditions
Problem is users trust them blindly without knowing their limits
So there is a need to test and compare how managers respond on phishing sites and find weak points

B. Objectives of the Research

1. To test and evaluate behaviour of different password managers on phishing websites
2. To compare browser based managers (Chrome Firefox) with standalone managers (Bitwarden, Lastpass , Keepassxc, Proton Pass)
3. To identify cases where managers autofill credentials on fake pages

C. Significance of the Study

1. Helps users to know how safe their password manager really is

2. Help the password manager developers make better systems by showing them vulnerabilities in the system.
3. Spreads awareness that password managers are not perfect and users must be careful

II. RELATED WORK

Past studies have studied password managers checking how safe they are and ease of use, how users use them. However, very few directly test them against phishing pages.

A. Survey Studies

1. Bimal Krishna, Arun Arya, AnanthaKrishna, Reeny Zakarias, Sanam E Anto, "Survey on Password Managers," International Journal of Advance Research (IJARIIE), 2025. This study explained features and usability, and mentioned passwordless as the future, but did not test phishing.
2. Nora Alkaldi & Karen Renaud, "Why Do People Adopt, or Reject, Smartphone Password Managers?," EuroUSEC, Jul 2016. Found that users avoid managers due to low trust and difficulty, focusing on behaviour rather than technical flaws.
3. Hussain Alshahrani, Abdulrahman Alghamdi, "The Factors Influencing the Use of Password Managers," JISCR, Jun 2022. described, using survey data, how usefulness and ease of use impact adoption.

B. Security and Vulnerability Studies

1. David Silver, Suman Jana, Dan Boneh, Eric Chen, Collin Jackson, "Password Managers: Attacks and Defenses," USENIX Security Symposium, Aug 2014. Showed autofill weaknesses but it is an older study.
2. Sean Oesch and Scott Ruoti, "That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers," USENIX Security Symposium, Aug 2020. Tested 13 browser-based managers and found autofill issues, but no phishing tests.
3. Petr Gallus, Dominik Staněk, Ivo Klaban, "Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions," International Conference on Cyber Warfare and Security (ICCWS), Mar 2025. Performed brute force and phishing-related tests but not on real phishing sites.
4. Andrés Fábrega, Armin Namavari, Rachit Agarwal, Ben Nassi, Thomas Ristenpart, "Exploiting Leakage in Password Managers via Injection Attacks," arXiv, Jan 2023. Showed leakage through injection attacks, not phishing.

C. Usability and User Behaviour

1. Timothy Sean Oesch, "An Analysis of Modern Password Manager Security and Usage on Desktop and Mobile Devices," University of Tennessee, May 2021. Found that built-in users prefer convenience while standalone users prefer safety.
2. Hirak Ray, Flynn Wolf, Ravi Kuber, "Why Older Adults (Don't) Use Password Managers," USENIX, Aug 2021. Found older users like managers but do not trust cloud storage.
3. Adryana Hutchinson, Jinwei Tang, Adam J. Aviv, Peter Story, "Measuring the Prevalence of Password Manager Issues Using In-Situ Experiments," NDSS Symposium, Feb 2024. Showed weaknesses in autofill and risky user habits.

D. Phishing and Mitigation Studies

1. Bilal Naqvi, Kseniia Perovaa, Ali Farooqb, Imran Makhdoomd, Shola Oyedeji, Jari Porras, "Mitigation Strategies Against the Phishing Attacks," Elsevier, Jul 2023. Reviewed many defenses but no password manager experiments.
2. Anuj Gautam, Tarun Kumar Yadav, Kent Seamons, Scott Ruoti, "Passwords Are Meant to Be Secret: A Practical Secure Password Entry Channel for Web Browsers," arXiv, Feb 2024. Proposed secure autofill but only proof of concept, not full evaluation.

III. METHODOLOGY

Tests were performed in a controlled environment using VirtualBox with a Windows 10 operating system image. No actual users, no active attacks, just test accounts and local configuration

A. Environment

• VirtualBox vm running windows 10. As a result, tests remain secure and separate from the internet and main system.
• Manual testing.
• Local server used (XAMPP) to host phishing pages.

B. Overall approach

Two methods were used to simulate phishing pages and test password managers. One methods is local and controlled so no internet hosting or targeting real people. And other is done using simulated phishing pages on Caniphish website.

C. Method 1 — Caniphish (simulated webpages)

• Caniphish was used to load and serve simulated phishing webpages provided by Caniphish templates.
• Researchers used Caniphish template pages as is.
• Test accounts (dummy usernames and passwords) were prepared and stored in each password manager under original domain names for realistic autofill behaviour.
• Tests were performed by opening the Caniphish page in the browser inside vm and observing whether the password manager autofilled, showed warning, or did nothing. Results were noted manually.
• Caniphish method gives quick realistic templates without needing to build pages from scratch.

D. Method 2 — hosts file trick with XAMPP (windows)

• The Windows 10 virtual machine had a local XAMPP server (Apache) installed. HTML pages that were phishing were made.
• To replicate actual domain names locally, hosts file mapping was employed.
• The local XAMPP page loads when the mapped URL is opened in the virtual machine browser after mapping, and the URL seems to be a real domain. This helps testing the behavior of password managers on realistic domain names.
• Tests were done manually: researcher opened each fake page, observed whether the password manager autofilled, showed warning, or blocked, etc results recorded in a table.

E. Password managers tested (as part of setup)

Tests included both browser built-in managers and standalone managers (Chrome, Firefox , Bitwarden, Lastpass , Keepassxc, Proton Pass). Each manager was installed inside the vm and configured with dummy credentials.

F. Test procedure (same for both methods)

1. In the password manager, set up a fake account credential and store it using the actual site domain (for example, `username@test` for `www.gmail.com`)
2. Open the Caniphish landing page or XAMPP hosted page in the browser within the virtual machine.
3. Examine how the password manager behaves.
4. Write the result down in a table.
5. Continue with various page styles (domain spoof, real).

G. Recording and gathering data

All observations are carefully entered into tables. Only dummy test accounts were used real credentials were not used.

H. Concerns about safety and ethics

• Only local servers were used in an isolated virtual machine environment for all studies. No actual users received any campaigns.
• Hosts file mapping kept everything on the local machine, no public hosting.

I. Limitations of this design

• Only Manual testing done so results depend on observation and may have human errors.
• Local hosting may not perfectly match all behaviours seen on real internet (especially https certificate handling) unless local https is configured.
• Only the chosen managers and page templates were tested, results may differ with other managers or more advanced phishing tricks.

IV. RESULTS AND ANALYSIS

The results are divided in two parts based on the two methods used in this study. The first method used Caniphish simulated phishing pages, and the second method used locally hosted pages via host

file trick with XAMPP. All the observations were taken manually inside the virtual machine and written in tables. No automation or scripts were used, only simple manual testing to see what password managers actually do when faced with phishing.

A. Results from Caniphish simulated pages:

The simulated pages included Facebook, Google, Instagram, LinkedIn, Microsoft and Zoom. These were directly loaded from Caniphish.

TABLE I
BEHAVIOR OF STANDALONE PASSWORD MANAGERS ON CANIPHISH PAGES:

Simulated page	**Password Managers**				
	Bitwarden	**Lastpass**	**Keepassxc**	**Proton Pass**	**Notes/Remarks**
Facebook	No autofill	No autofill	Manual fill	No autofill	Most managers recognize the URL; behavior is based on domain.
Google	No autofill	No autofill	Manual fill	No autofill	Most managers recognize the URL; behavior is based on domain.
Instagram	No autofill	No autofill	Manual fill	No autofill	Most managers recognize the URL; behavior is based on domain.
LinkedIn	No autofill	No autofill	Manual fill	No autofill	Most managers recognize the URL; behavior is based on domain.
Microsoft	No autofill	No autofill	Manual fill	No autofill	Most managers recognize the URL; behavior is based on domain.
Zoom	No autofill	No autofill	Manual fill	No autofill	Most managers recognize the URL; behavior is based on domain.

TABLE II
BEHAVIOR OF BROWSER BUILT-IN PASSWORD MANAGERS ON CANIPHISH PAGES:

Simulated page	**Password Managers**				
	Chrome	**Firefox**	**Brave**	**Egde**	**Notes/Remarks**
Facebook	Asks for manual fill	Suggests username, no autofill	Asks for manual fill	Autofills email only	Doesn't recognise url; common issue across browsers is the URL structure of the test page
Google	Asks for manual fill	No autofill	Asks for manual fill	Autofills wrong email	Doesn't recognise url; common issue across browsers is the URL structure of the test page
Instagram	Asks for manual fill	No autofill	Asks for manual fill	Autofills wrong email	Doesn't recognise url; common issue across browsers is the URL structure of the test page
LinkedIn	Asks for manual fill	No autofill	Asks for manual fill	Autofills wrong email	Doesn't recognise url; common issue across browsers is the URL structure of the test page
Microsoft	Asks for manual fill	No autofill	Asks for manual fill	Autofills wrong email	Doesn't recognise url;
Zoom	Asks for manual fill	No autofill	Asks for manual fill	Autofills wrong email	Doesn't recognise url;

Analysis:

• Most browser based managers (Chrome, Firefox , Brave) did not autofill credentials, instead they either asked for manual fill or just refused to provide data.

• Edge behaved differently, in many cases it autofilled only partial data like email but not the full login. This shows inconsistency.

• Standalone managers like Bitwarden, Lastpass , Proton Pass mostly refused to autofill. Keepassxc only allowed manual fill, which means the user had to copy paste.

• Overall result from Caniphish: the managers showed safe behavior in most cases. Autofill rarely happened, and majority blocked or required manual action.

B. Results from XAMPP + Hosts File Trick:

In this method the pages like Canva, Facebook, LinkedIn, and spoofed domains like canvaa.com or llinkedin.com were hosted locally

TABLE III
BEHAVIOR OF STANDALONE PASSWORD MANAGERS ON XAMPP HOSTED PHISHING PAGES:

Simulated page	**Password Managers**					
	Hosts Mapping Type	**Bitwarden**	**Lastpass**	**Keepassxc**	**Proton Pass**	**Notes/Remarks**
canva.com	Mapped via hosts	Site refused to load (certificate error)	Refused to load (certificate error)	Refused to load (certificate error)	Refused to load (certificate error)	HTTPS certificate mismatch due to hosts override.
canvaa.com	Domain Spoofing	No autofill	No autofill	Manual fill	No autofill	Domain differs, treated as a different site.
linkedin.com	Mapped via hosts	Site Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS certificate mismatch due to hosts override.
llinkedin.com	Domain Spoofing	No autofill	No autofill	Manual fill	No autofill	Domain differs, treated as a different site.
facebook.com	Mapped via hosts	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS certificate mismatch due to hosts override.
faceboook.com	Domain Spoofing	No autofill	No autofill	Manual fill	No autofill	Domain differs, treated as a different site.
etsy.com	Mapped via hosts	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS certificate mismatch due to hosts override.
eetsy.com	Domain Spoofing	No autofill	No autofill	Manual fill	No autofill	Domain differs, treated as a different site.

TABLE IV
BEHAVIOR OF BROWSER BUILT-IN PASSWORD MANAGERS ON XAMPP HOSTED PHISHING PAGES:

Simulated page	Password Managers					
	Hosts Mapping Type	Chrome	Firefox	Brave	Edge	Notes/Remarks
canva.com	Mapped via hosts	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS cert mismatch due to hosts override.
canvaa.com	Domain Spoofing	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill	Domain differs, treated as a different site.
linkedin.com	Mapped via hosts	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS cert mismatch due to hosts override.
llinkedin.com	Domain Spoofing	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill	Domain differs, treated as a different site.
facebook.com	Mapped via hosts	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS cert mismatch due to hosts override.
faceboook.com	Domain Spoofing	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill	Domain differs, treated as a different site.
etsy.com	Mapped via hosts	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	Site refused to load (certificate error)	HTTPS cert mismatch due to hosts override.
eetsy.com	Domain Spoofing	Shows warning, no autofill	Shows warning, no autofill	Shows warning, no autofill.	Shows warning, no autofill	Domain differs, treated as a different site.

C. Analysis:

• All browsers (Chrome, Firefox , Brave, Edge) refused to load mapped domains due to certificate mismatch. When spoofed domains were used, they showed warnings and did not autofill.

• Browser based managers showed more clear warnings here compared to Caniphish pages.

• Standalone managers also refused autofill in almost all cases. Bitwarden, Lastpass , Proton Pass showed no autofill, while Keepassxc again required manual copy paste.

• Overall result from XAMPP method: the certificate error created by hosts override was strong enough to stop autofill. Spoofed domains were treated as different sites, so autofill was avoided.

V. DISCUSSION

When comparing both methods, the behavior was quite consistent:

1. Managers avoided autofill in majority of phishing cases.
2. Edge browser manager showed the weakest behavior because it autofilled partial data in Caniphish pages, even though others blocked.
3. Keepassxc stood out as most strict since it never autofilled automatically, only allowed manual copy paste.
4. Certificate error and domain mismatch acted as strong natural protection.

These results suggest that password managers today are mostly safe against simple phishing attempts, but there are still small risks where partial autofill can happen. This shows that while users

should trust password managers, they also must stay aware that not all managers behave equally.

VI. Findings and Suggestions

This research was carried out to study how password managers behave when exposed to phishing websites. The testing was done using two safe methods, Caniphish simulated phishing pages and locally hosted phishing pages through the hosts file trick combined with XAMPP. All tests were done manually without automation. The results were noted in tables and then analyzed to understand the actual behavior of different managers. Drawing from the obtained data, the subsequent discoveries and recommendations are presented.

A. Findings

1. General effectiveness:

• Most password managers did not autofill credentials on phishing pages.

• When certification error was shown most browsers, blocked the site from loading and warned when using spoofed URLs.

• This shows that password managers are becoming stronger against common phishing attempts.

2. Browser based managers

• Chrome, Firefox and Brave showed safe behavior in almost all tests.

• They usually blocked autofill or displayed warnings when phishing domains were detected.

• Microsoft Edge was less consistent. In Caniphish pages, it autofilled partial information like email id which could still be misused by attackers.

3. Standalone managers

• Bitwarden, Lastpass and Proton Pass generally refused autofill on phishing pages.

• They did not leak any credentials even when domains looked similar.

• Keepassxc was the strictest manager, as it never autofilled automatically. The user had to manually copy and paste the login data. This reduced risk but also made it less convenient.

4. Phishing setup differences:

• In Caniphish, the pages loaded properly without certificate issues, which gave a real-world like experience. Here some managers like Edge behaved weakly.

• In XAMPP hosted phishing, certificate errors due to localhost mapping worked as a natural defense. Most managers blocked autofill completely.

• Spoofed domains (like canvaa.com or llinkedin.com) were treated as different websites by the managers, so autofill did not trigger.

B. Overall pattern

• Across both methods, autofill on phishing pages was rare but still possible.

• Edge showed the weakest results, while Keepassxc was the most secure.

• Other managers performed reasonably well but showed small differences in behavior.

C. Suggestions

1. for users:

• Users should not blindly trust password managers.

• Always check the website URL carefully.

• Implement multi-factor authentication when available, since it provides additional security protection beyond single-factor verification.

2. for developers of password managers

• Developers of Password managers should improve phishing detection by adding stronger domain matching and certificate checking.

3. for researchers:

• Future researchers should study password managers under more advanced phishing tricks such as using certified URLs with SSL certificates.

• User studies be done to understand how people react when their manager blocks autofill or if do they recognize the warning or ignore it.

VII. Conclusion and Future Work

The experimental evaluation conducted in this study demonstrates that password management tools typically succeed in preventing phishing attempts, though they are not without limitations. There are still minor cases where partial data is

leaked or warnings may not be clear enough for the user. Results show that password managers while can provide you good security users too have to be careful when you are on the internet.

The suggestions made here can help users be more secure, and also help the password manager developers make better systems.

For future work, researchers can test with larger datasets, use advanced phishing and study real-world user reactions. This would provide more complete knowledge on how password managers behave in practice and how they can be further improved.

VIII. REFERENCES

[1] B. Krishna, A. Arya, A. Krishna, R. Zakarias, and S. E. Anto, "Survey on Password Managers," International Journal of Advance Research (IJARIIE), 2025.

[2] N. Alkaldi and K. Renaud, "Why Do People Adopt, or Reject, Smartphone Password Managers?," EuroUSEC, Jul. 2016.

[3] H. Alshahrani and A. Alghamdi, "The Factors Influencing the Use of Password Managers," JISCR, Jun. 2022.

[4] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password Managers: Attacks and Defenses," USENIX Security Symposium, Aug. 2014.

[5] S. Oesch and S. Ruoti, "That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers," USENIX Security Symposium, Aug. 2020.

[6] P. Gallus, D. Staněk, and I. Klaban, "Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions," International Conference on Cyber Warfare and Security (ICCWS), Mar. 2025.

[7] A. Fábrega, A. Namavari, R. Agarwal, B. Nassi, and T. Ristenpart, "Exploiting Leakage in Password Managers via Injection Attacks," arXiv, Jan. 2023.

[8] T. S. Oesch, "An Analysis of Modern Password Manager Security and Usage on Desktop and Mobile Devices," University of Tennessee, May 2021.

[9] H. Ray, F. Wolf, and R. Kuber, "Why Older Adults (Don't) Use Password Managers," USENIX, Aug. 2021.

[10] A. Hutchinson, J. Tang, A. J. Aviv, and P. Story, "Measuring the Prevalence of Password Manager Issues Using In-Situ Experiments," NDSS Symposium, Feb. 2024.

[11] B. Naqvi, K. Perovaa, A. Farooqb, I. Makhdoomd, S. Oyedeji, and J. Porras, "Mitigation Strategies Against the Phishing Attacks," Elsevier, Jul. 2023.

[12] A. Gautam, T. K. Yadav, K. Seamons, and S. Ruoti, "Passwords Are Meant to Be Secret: A Practical Secure Password Entry Channel for Web Browsers," arXiv, Feb. 2024.

IX. APPENDIX

Appendix A: Tools Used

- Caniphish platform (for simulated phishing pages)
- XAMPP server (for local hosting)
- Hosts file override (for domain redirection)
- Browsers: chrome, Firefox, brave, edge
- Standalone Password Managers: Bitwarden, Lastpass, Proton Pass, Keepassxc

Appendix B: Observation Tables

Table I: Behavior of Standalone Password Managers on Caniphish Pages.

Table II: Behavior of Browser Built-in Password Managers on Caniphish Pages

Table III: Behavior of Standalone Password Managers on XAMPP Hosted Phishing Pages

Table IV: Behavior of Browser Built-in Password Managers on XAMPP Hosted Phishing Pages

Appendix C: Virtual Machine Setup

Fig. C1. VirtualBox settings used for the experiment (windows 10 iso inside virtual machine).

Appendix D: Experimental Setup and Screenshots

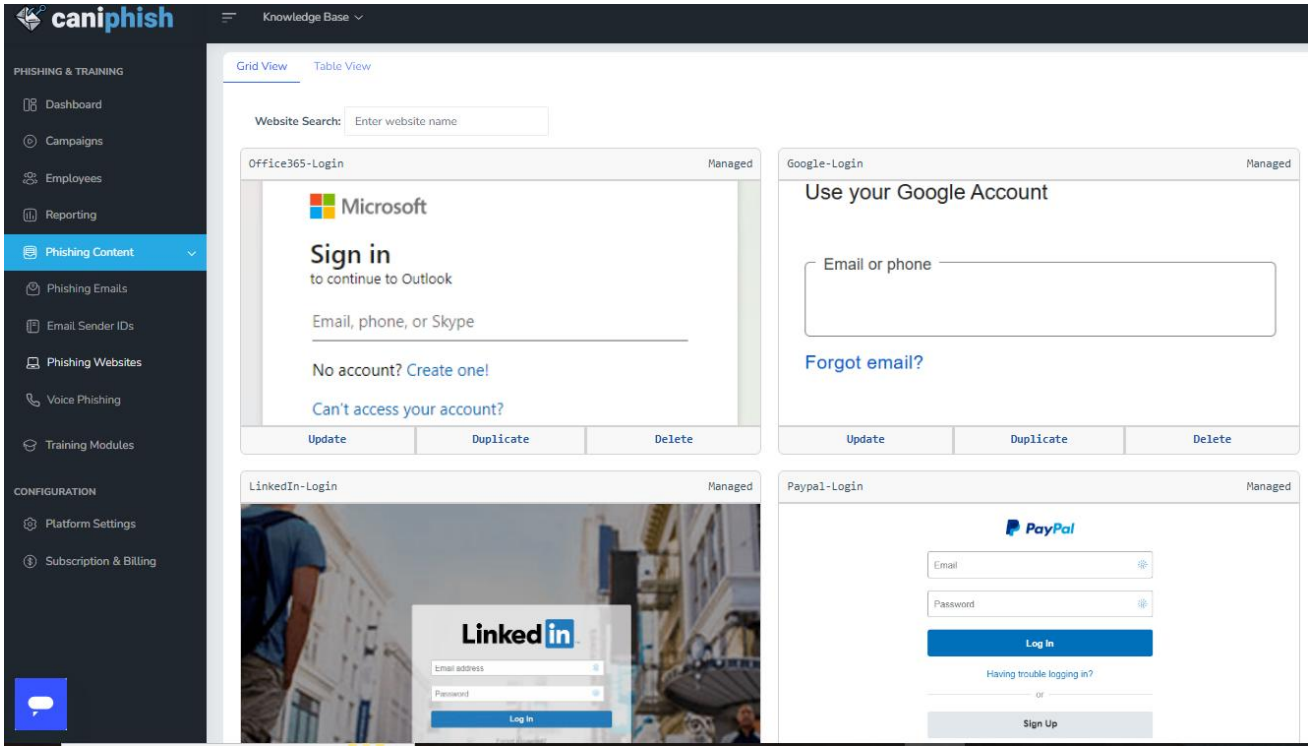

Fig. D1. Caniphish templates Dashboard

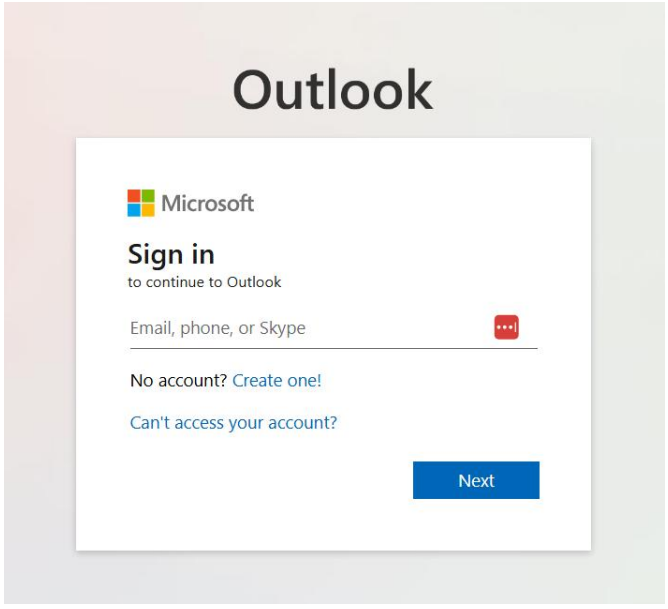

Fig. D2. Caniphish example template Microsoft login page used in tests.

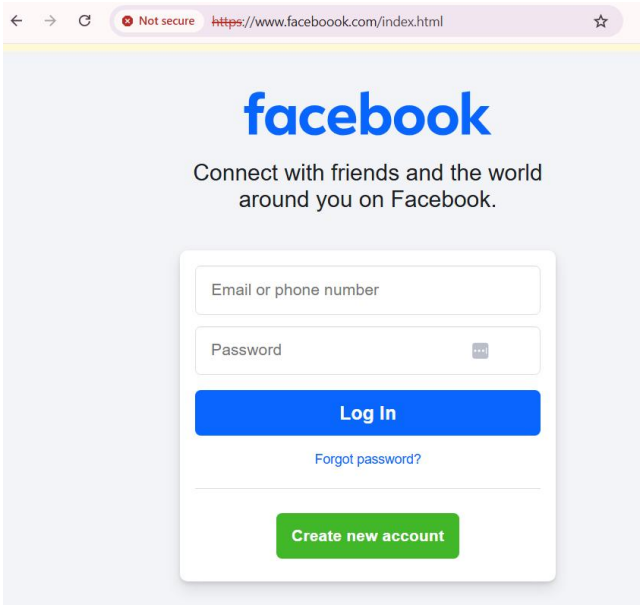

Fig. D3. XAMPP hosted spoofed site (faceboook.com)

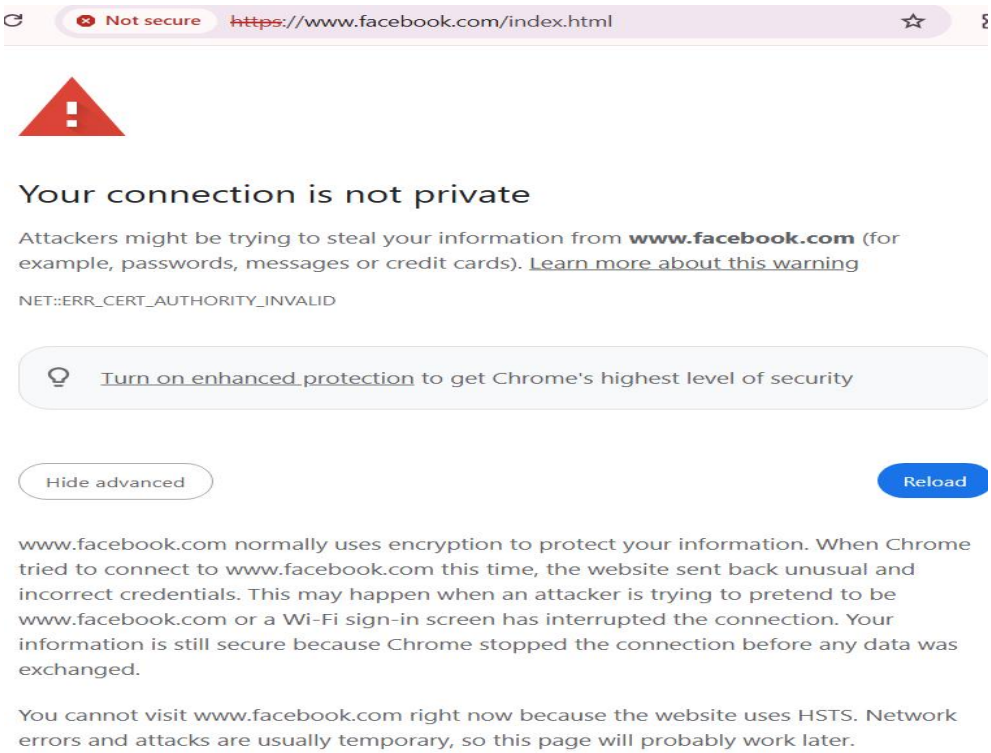

Fig. D4. Browser refusing to load site XAMPP hosted site (Facebook.com)

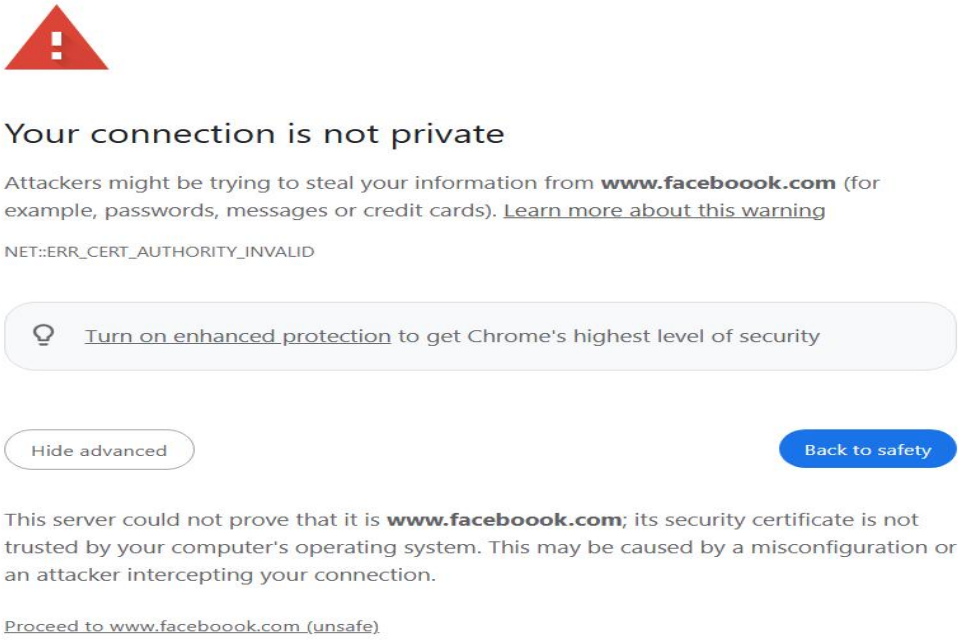

Fig. D5. Browser showing warning on XAMPP hosted spoofed site (Faceboook.com)