Hosting Phishing sites

Phishing attack is a type of social engineering attack. It is client-based attack. It is used to steal user data, including login credentials and credit card numbers, etc. It is a cybercrime in which targets are contacted by email, telephone or text message.

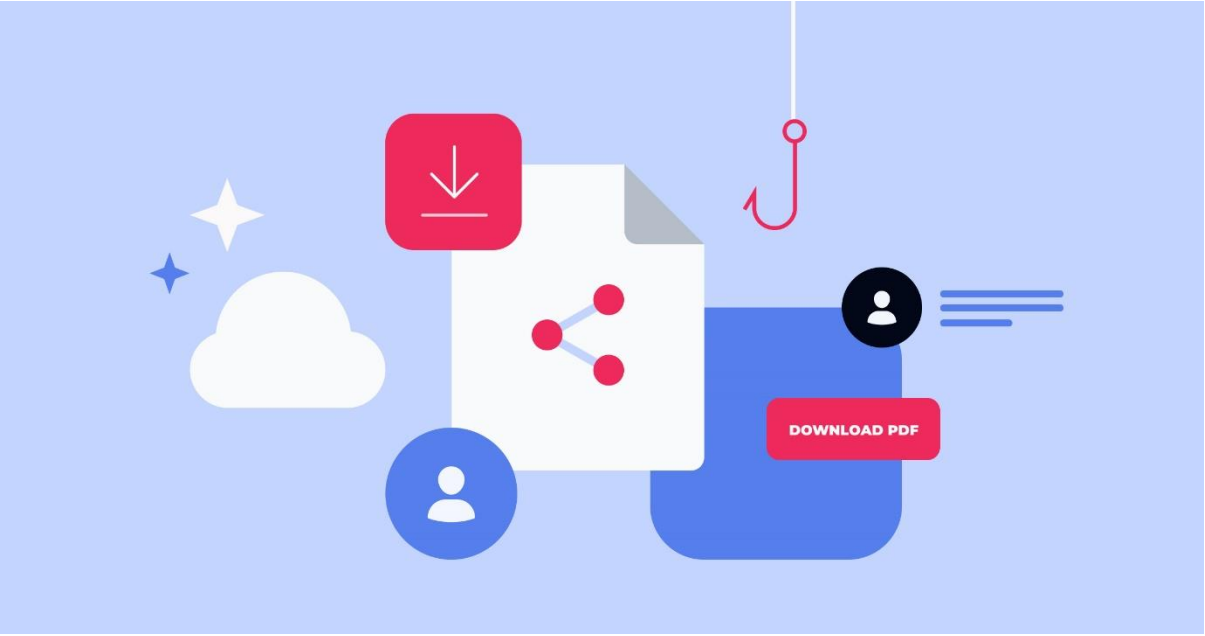
Phishing is done by using the methods-

- Redirection using local host
- Redirection using server
- Base-64 encoding
- Host file manipulation
- Full screen API

There are various phishing tools are designed to create phishing websites for various platforms like Instagram, Facebook, You Tube, etc. Now-a-days more and more cybercriminals are using abusing legitimate software-as-a-service (SaaS) platforms to host their phishing pages. As these URLs are hosted on legitimate domains, they can be difficult to detect for phishing detection engines.

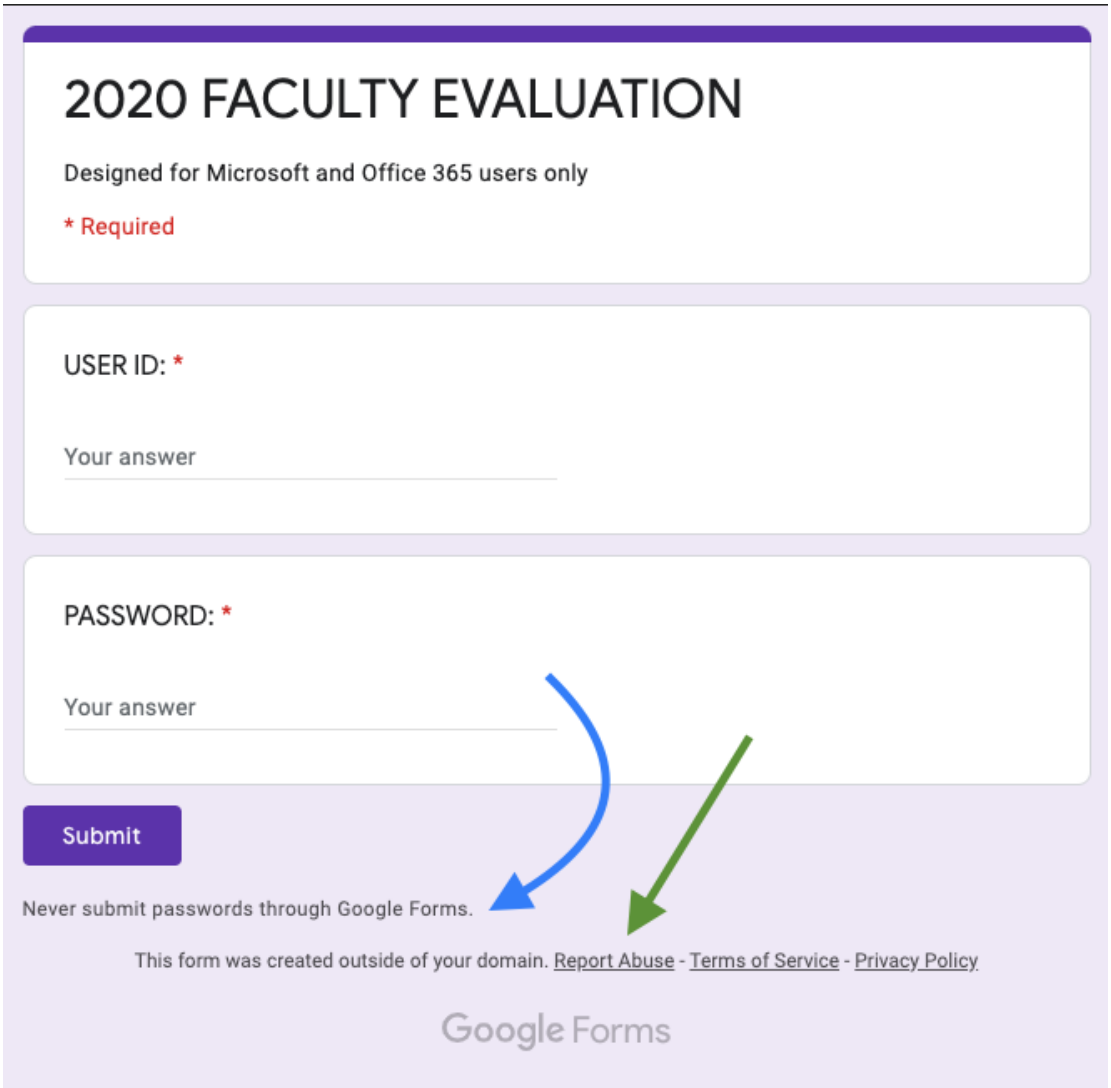
From the beginning of 2020 to June 2022, it is observed that the number of phishing URLs hosted on legitimate SaaS platforms has continued to increase at an alarming rate. In fact, the rate of newly detected phishing URLs hosted on legitimate SaaS platforms has increased over 1100% from June 2021-June 2022.

File Sharing-



Most of attackers use file sharing sites because these sites offer users the ability to grant access to view, add, and edit files already stored on the cloud drive. Users are first asked to access these resources. After giving the permissions to the attack by user, an attacker now can view any files on the file-sharing resource and add new ones. These new files usually contain malicious scripts which could add malware to the local machine, steal credentials, access personal data or give the attacker the ability to control the user's remote device. By using this attack, an attacker has permissions to add the file again so deleting the malicious file will not stop the attack.

Form Builders-



There are several sites are used to create forms for phishing. They are as follows.

- 123formbuilder.com
- docs.google.com
- form.simplesurvey.com
- formpl.us
- forms.gle
- forms.office.com
- formtools.com
- smartsurvey.co.uk
- supersimplesurvey.com
- survey.survicate.com

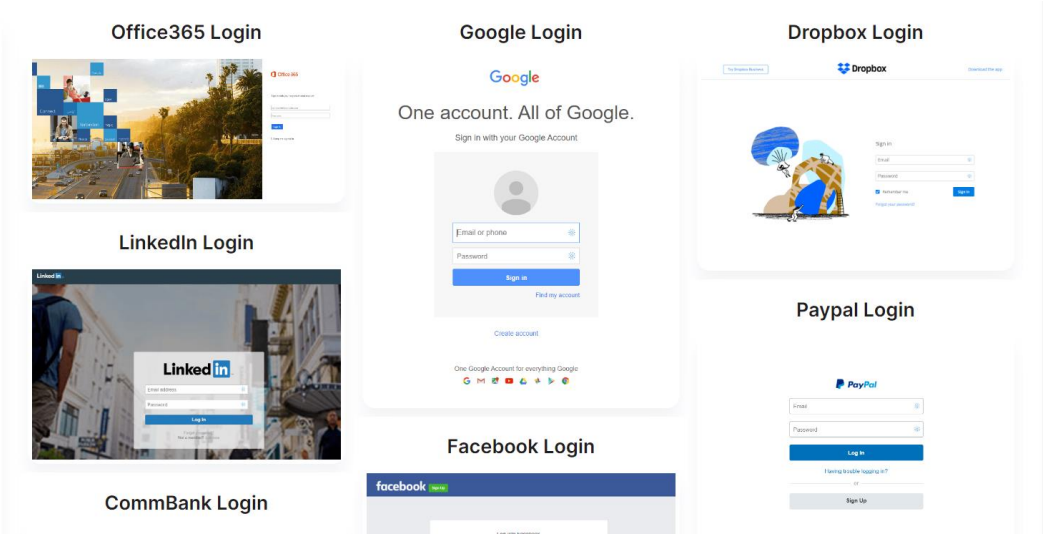
- surveygizmo.com
- survs.com
- zfrmz.com

Cybercriminals can create forms in these sites without any programmable knowledge. These pages are then propagated through emails. Microsoft Forms site is the same vendor as Outlook, so a common form builder used form emails is Microsoft Forms by an attacker. Super Simple Survey is commonly used as well.

Website Builders-

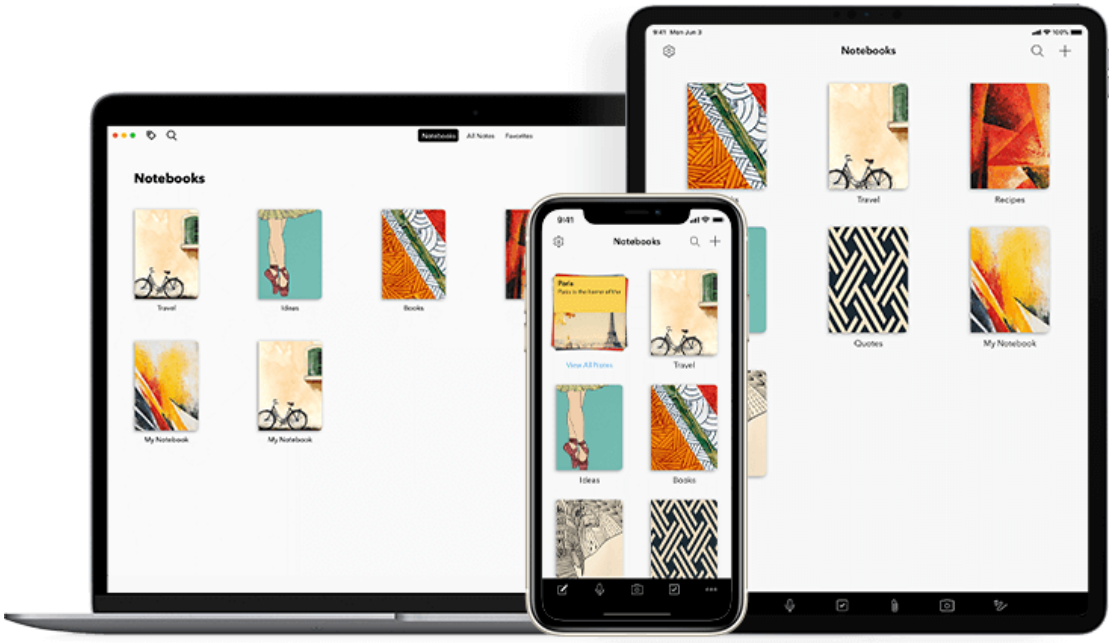
Phishing websites typically designed to steal or gather sensitive information from a target. This includes credential harvesting or theft of credit card information. By combining phishing websites with phishing emails, an attacker does phishing. Phishing emails are used as the initial mechanism to trick a user into landing on a phishing website. To allure targets into providing their sensitive data the attacker needs to masquerade as a legitimate service.

Weebly is a popular site-building which offers users a simple drag-and-drop interface for creating websites. Weebly has also been used by scammers and phishers to create fake websites in order to steal personal information or login credentials and other sensitive information.



Note Taking/Collaboration-

Out of the last 1,430 most recent emails it observed that 95.5% of links were created for phishing purposes. Scammers have been sending emails containing a link to a page from note-taking app, this page leads to a second link. On clicking that link, user directs to a phishing page.



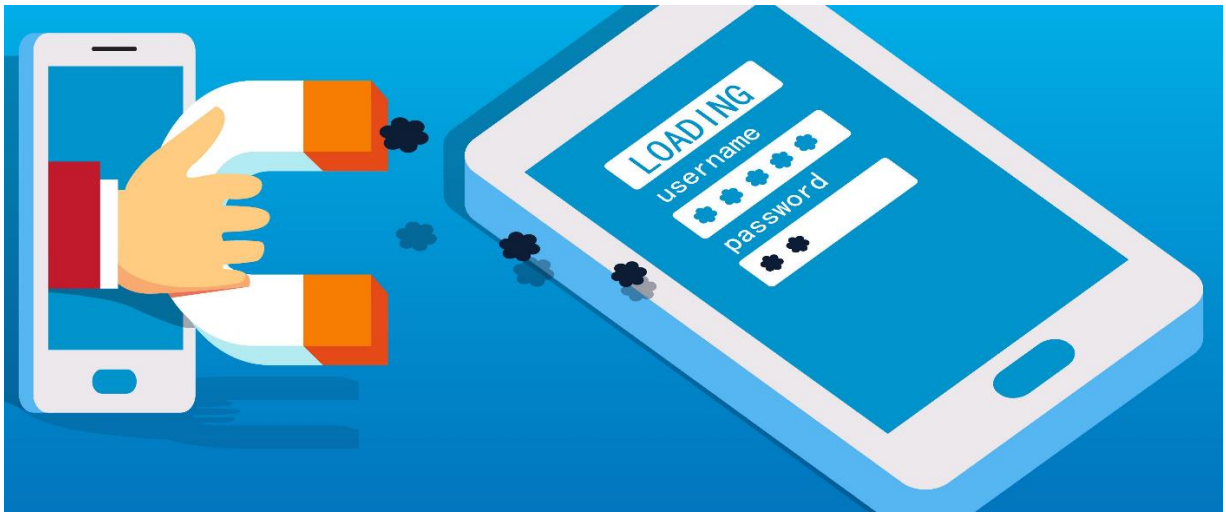
Brand impersonation-

Brand impersonation involves the use of a brand name, logo, legitimate-looking emails and websites into tricking the user into clicking on links without sending spoofed emails to a target. By using this technique, an attacker steal credentials. Below is the top 10 list of brands most impersonated in phishing campaigns:

- Microsoft
- PayPal
- Facebook
- Netflix
- Bank of America

- Apple
- CIBC
- Amazon
- DHL
- DocuSign

In brand impersonation users have received an email from a reputable brand. When they click link, it will lead the user to a landing page with the brand logo to change their password in order to capture login credentials to the brand's legitimate website and after this an attacker steal all the information entered by user.



Design/Prototyping-

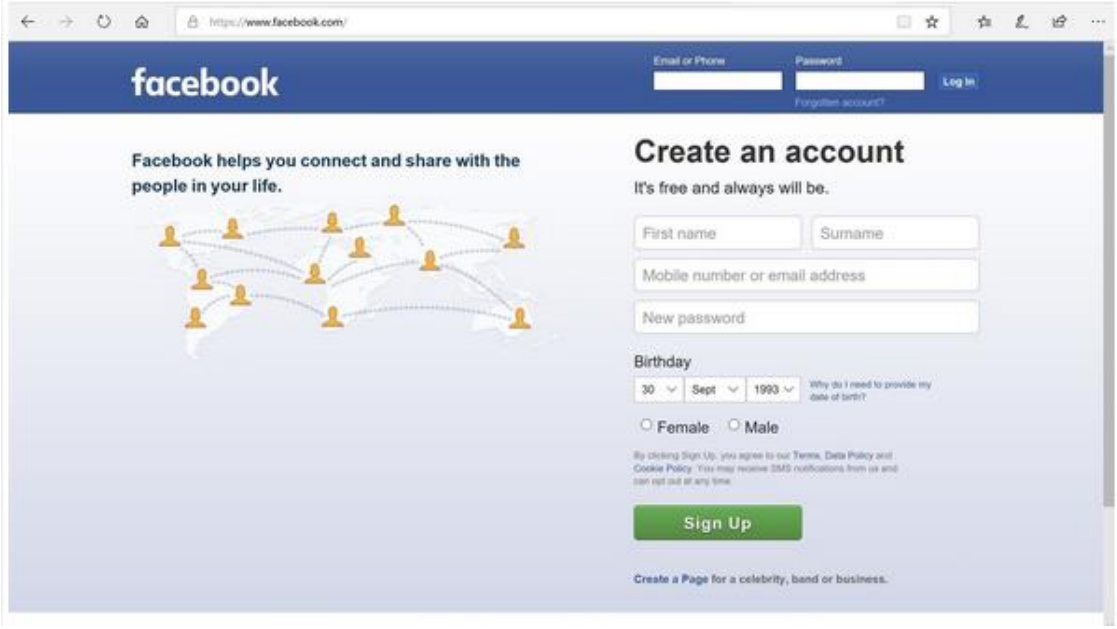
Prototyping is a process of implementing ideas into tangible forms from paper to digital. With prototypes, one can refine and validate designs so the brand can release the right products. An attacker creates high-fidelity mobile prototypes which look and work as a real app. By using this technique, an attacker launches phishing attacks because this technique is very cheap and fast.

Process to create and host phishing site:

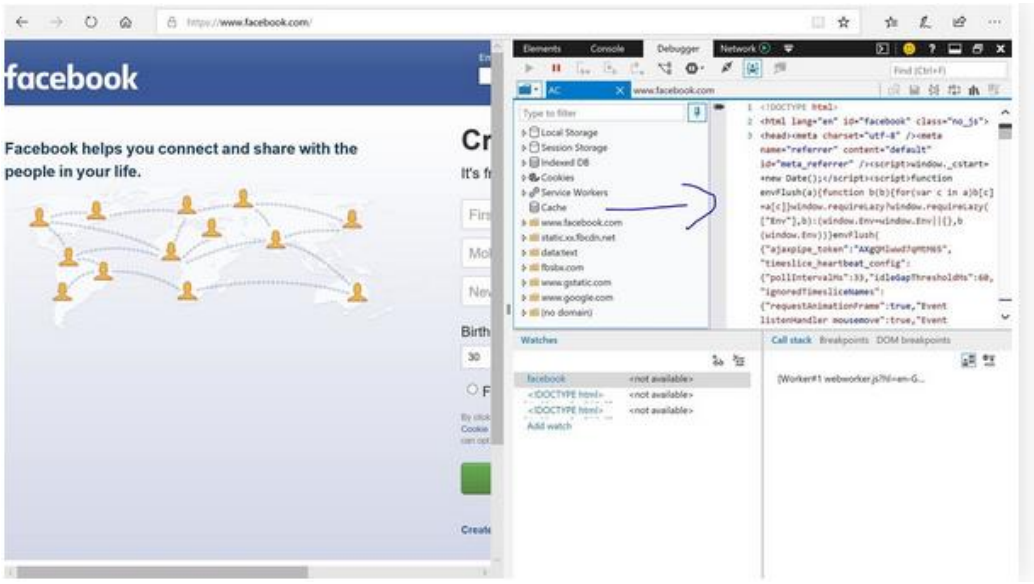
Local host is the default name of the computer i.e., 127.0.0.1 which is also called as loop back address. XAMPP is the most popular PHP development environment which build an easy to install distribution for developers to get into the world of Apache. To access the server, you need to install XAMPP in the system. You can also download localhost Wamp Server. Once you open XAMPP, control page can be open. Start Apache server which make your system act as web server.

The web server is responsible for handling the requests and responses. When you searched for any URL in browser, the request is handled by DNS server which translates host name in IP address and sends it to respective server. The server has many files from which default file is fetched as a response. Similarly, when we type localhost in a browser, the request is handled by the same server which is running in a same system. This shows XAMPP page as a response. When this page is replaced by phishing page, we get the response is the phishing page. So, how can we create this phishing page?

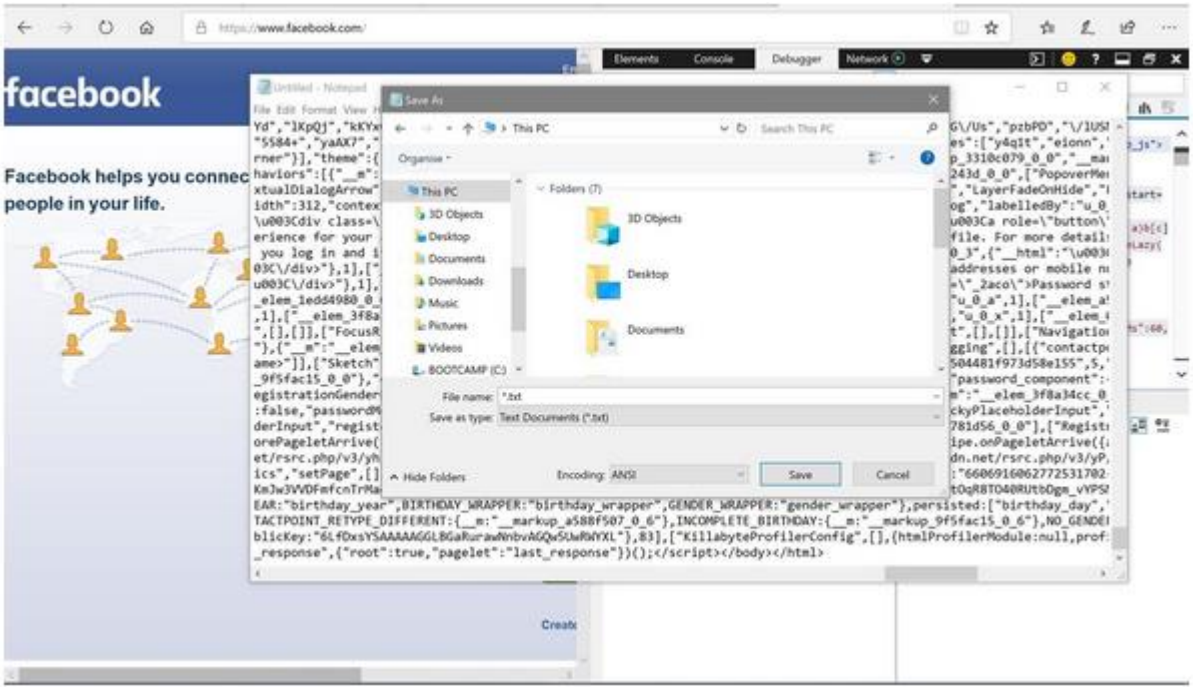
1) Here, we are going to make phishing webpage of Facebook. For this, you have to download the HTML index of the target webpage. Now navigate to webpage.



View the sources of the webpage.

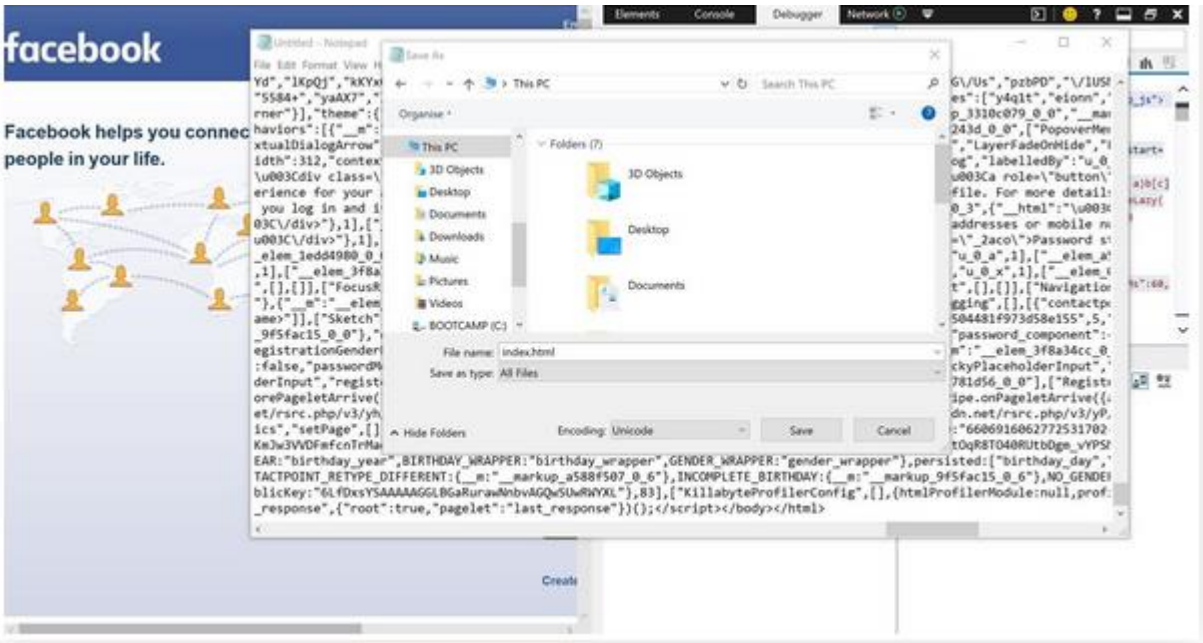


Now download and save source code.

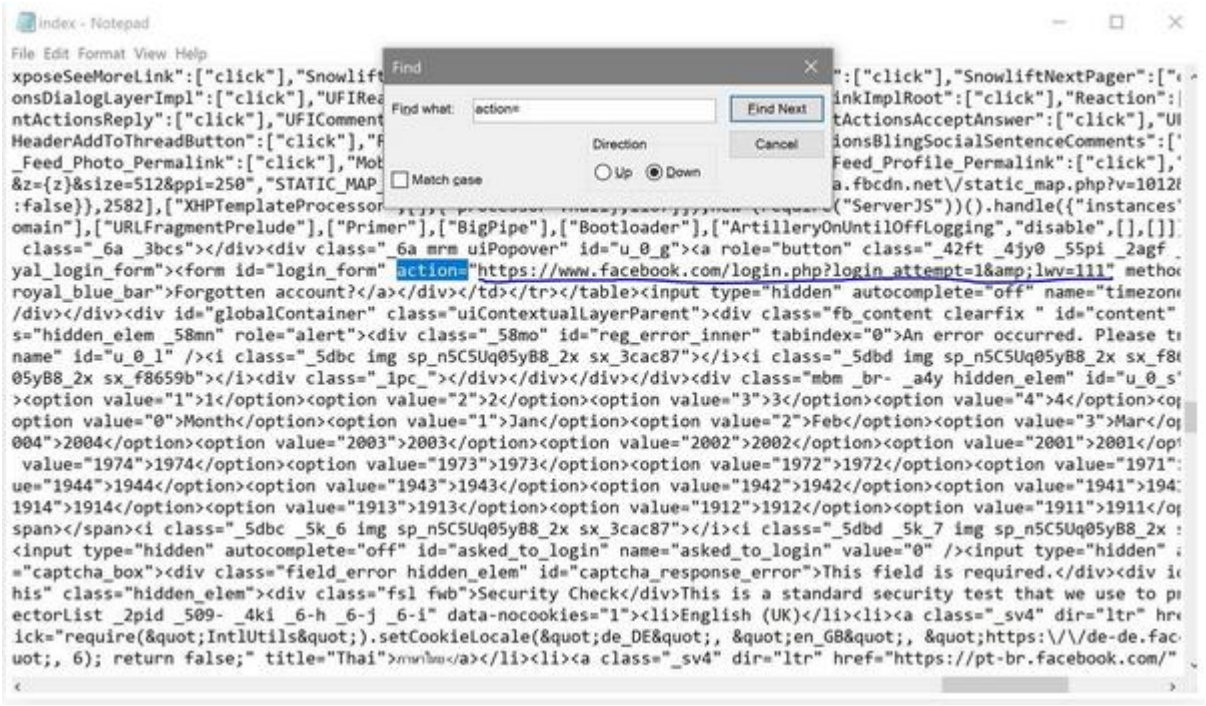


Change "Save as type" to All Files and change the encoding to Unicode.

After that, name the document "index.html"



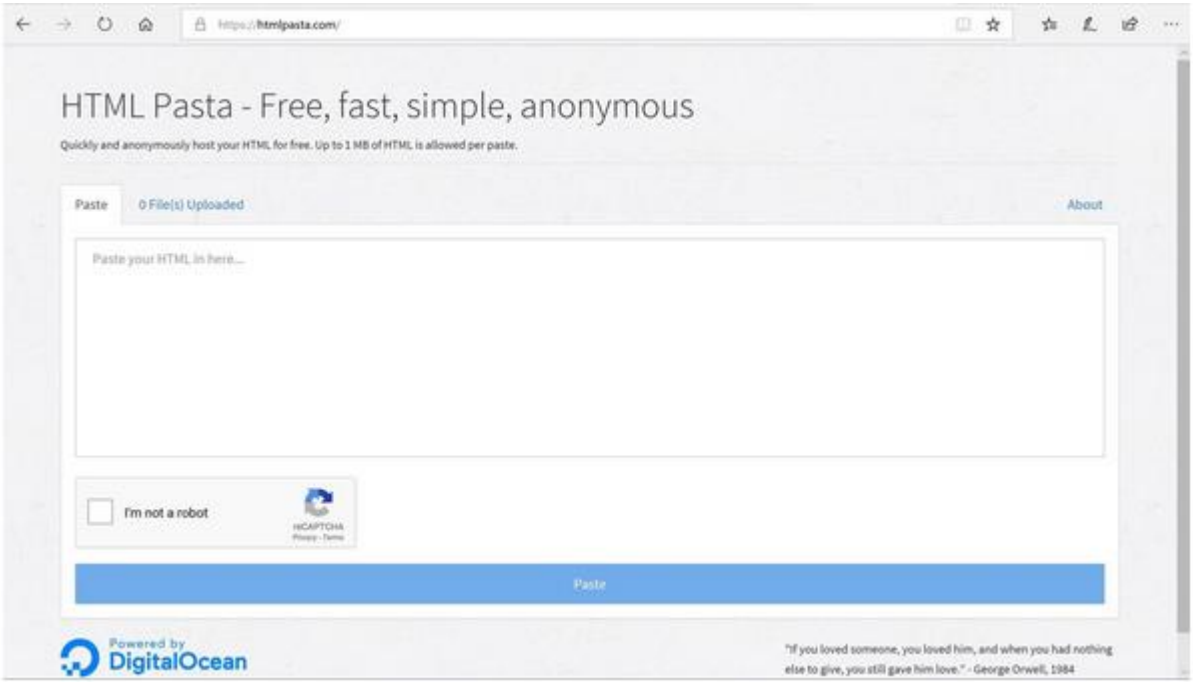
2) Now Create a PHP File for password harvesting which harvests the user's password.
3) Now, incorporate PHP file, to receive passwords that the users send.



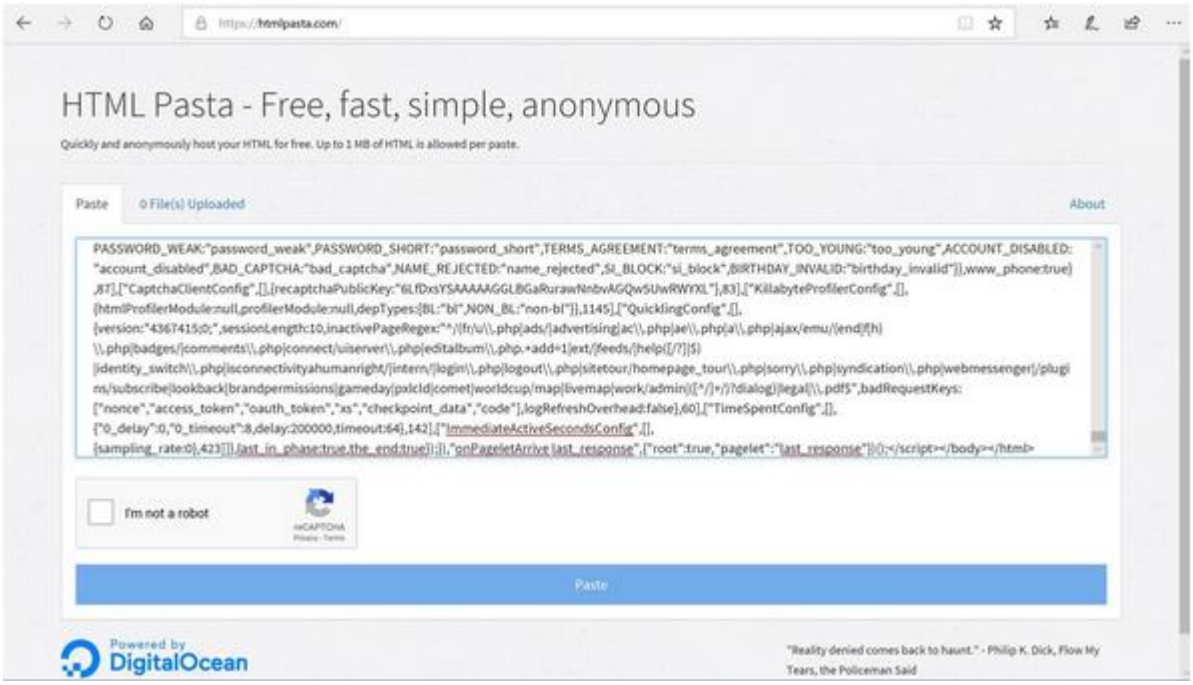
Press Ctrl-F and type "=action" in the field. Replace underlined portion with "post.php" with keeping the speech marks.

By using any free hosting services to host and store passwords. Navigate to the FTP Server for Web Hosting Service.

4) For hosting actual page navigate htmlpasta.com.



Copy the index.html file for phishing site and paste it in here.



After clicking on the reCAPTCHA and paste, you will get a link for website.

Now the phishing page is ready.

Now when the other systems within the network access the localhost phishing page will get open. After inserting credentials, it will save in the file. This is how phishing works.

References:

https://unit42.paloaltonetworks.com/platform-abuse-phishing/

https://xd.adobe.com/ideas/process/ui-design/what-is-prototyping/

https://www.mailguard.com.au/blog/creatives-beware-file-sharing-service-wetransfer-used-in-fresh-phishing-scam

https://blog.cleantalk.org/visual-form-builder-contact-form

https://yanngirard.typepad.com