

# New Phishing toolkit lets anyone create fake Chrome browser windows

---

[bleepingcomputer.com/news/security/new-phishing-toolkit-lets-anyone-create-fake-chrome-browser-windows/](https://bleepingcomputer.com/news/security/new-phishing-toolkit-lets-anyone-create-fake-chrome-browser-windows/)

Lawrence Abrams

By

[Lawrence Abrams](#)

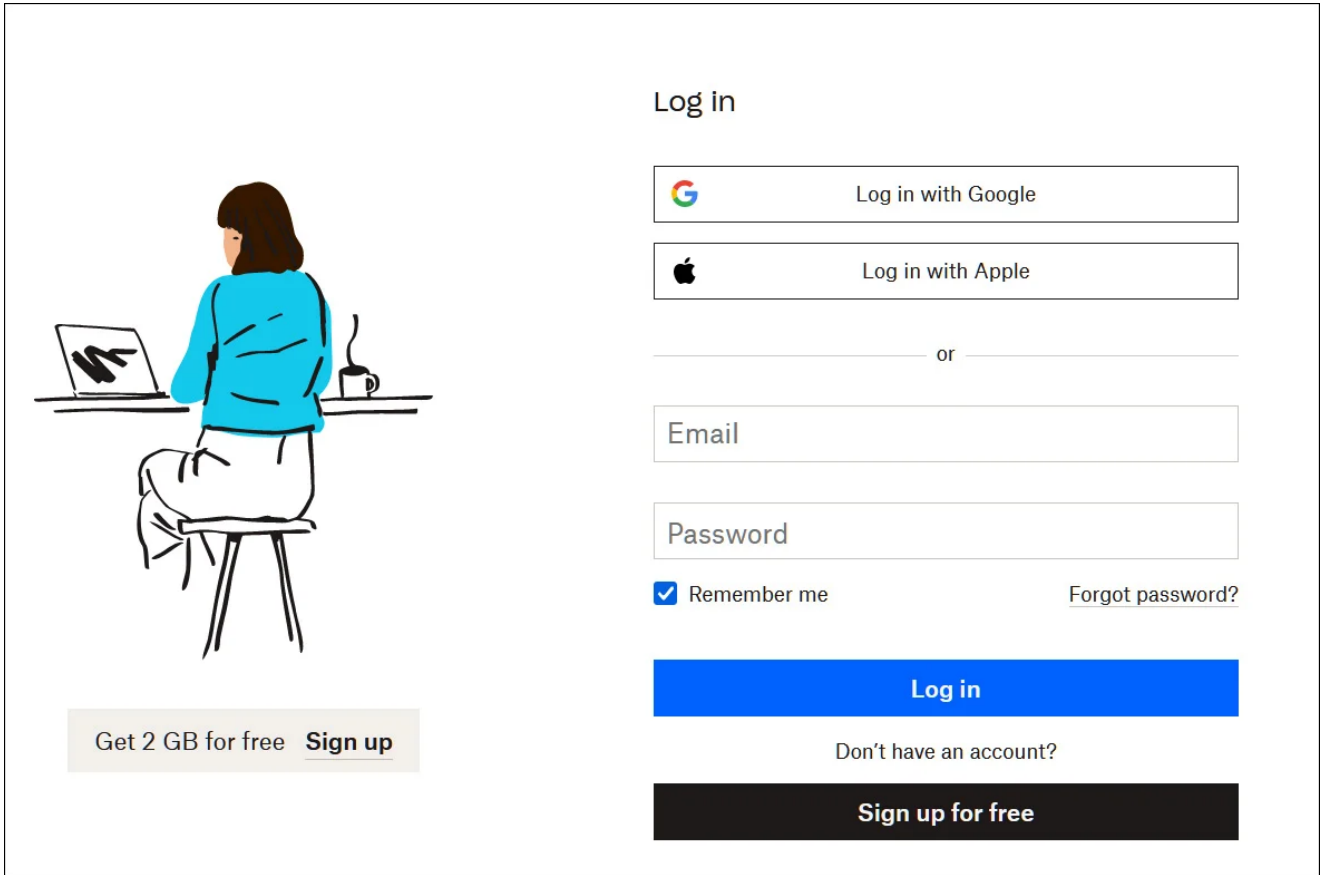
- March 19, 2022
- 11:16 AM
- 0



A phishing kit has been released that allows red teamers and wannabe cybercriminals to create effective single sign-on phishing login forms using fake Chrome browser windows.

When signing into websites, it is common to see the option to sign with Google, Microsoft, Apple, Twitter, or even Steam.

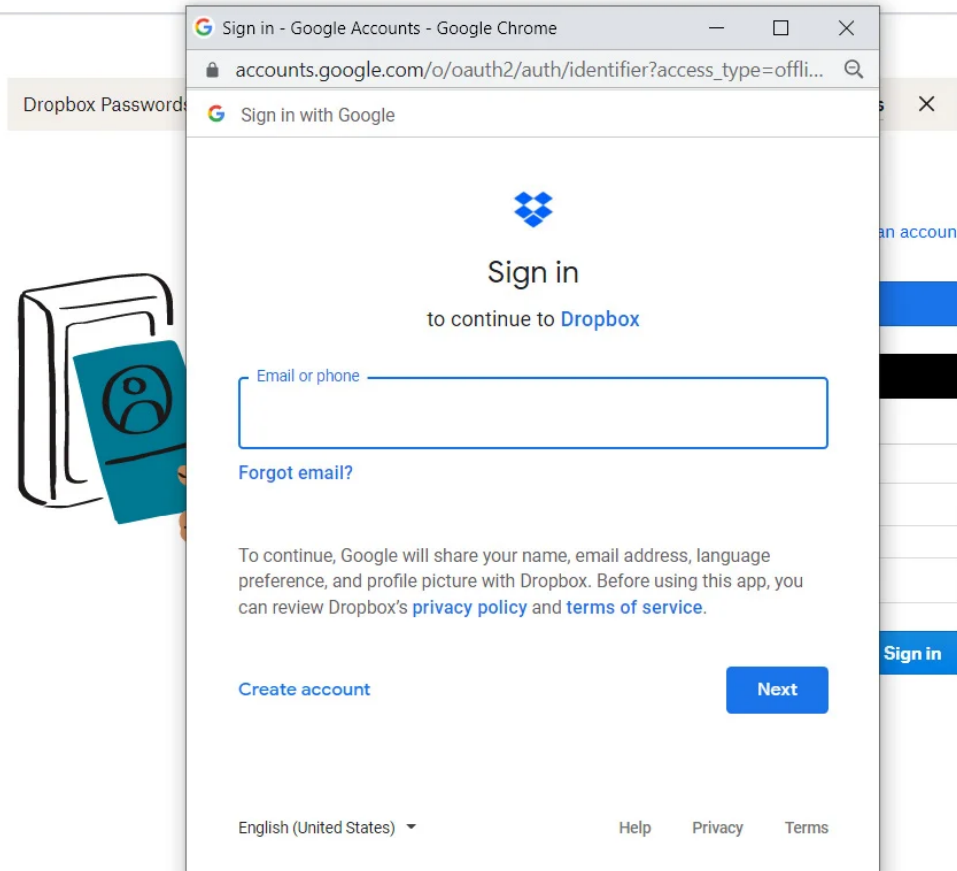
For example, the login form for DropBox allows you to login using an Apple or Google account, as shown below.



### DropBox login form

When clicking the Login in Google or App buttons, a single-sign-on (SSO) browser window will be displayed, prompting you to enter your credentials and login with the account.

These Windows are stripped down to only show the login form and an address bar showing the URL of the login form.



### Legitimate sign in with Google window

While this address bar is disabled in these SSO windows, you can still use the displayed URL to verify that a legitimate google.com domain is being used to sign you into the site. This URL further adds to the trust of the form and will make you feel comfortable entering your login credentials.

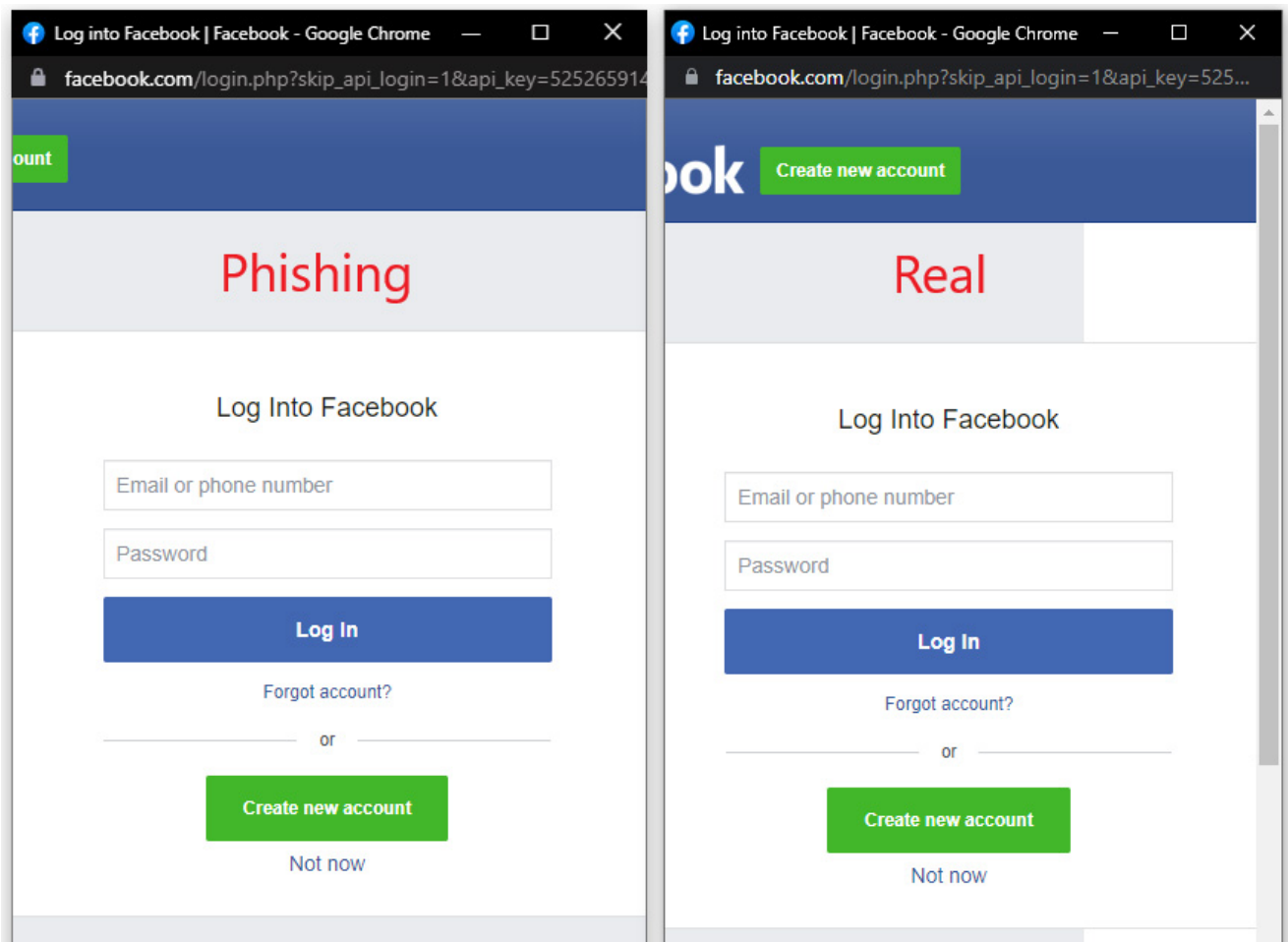
Threat actors have attempted to create these fake SSO windows using HTML, CSS, and JavaScript in the past, but there is usually something a little off about the windows, making them look suspicious.

### Introducing Browser in the Browser attacks

This is where a new "Browser in the Browser (BitB) Attack" comes into play that uses premade templates to create fake but realistic, Chrome popup windows that includes custom address URLs and titles that can be used in phishing attacks.

Basically, this attack creates fake browser windows within real browser windows (Browser in the Browser) to create convincing phishing attacks.

The Browser in the Browser attack templates was created by security researcher mr.d0x, who released the templates on GitHub. These templates include those for Google Chrome for Windows and Mac and dark and light mode variants.



### Example BitB Chrome phishing windows for Facebook

Source: *mr.d0x*

mr.d0x told BleepingComputer that the templates are very simple to use in creating convincing Chrome windows to display single sign-on login forms for any online platform.

The researcher said that redteamers could simply download the templates, edit them to contain the desired URL and Window title, and then use an iframe to display the login form.

It is also possible to add the HTML for the login form directly into the template, but mr.d0x told BleepingComputer that you would need to align the form properly using CSS and HTML.

Kuba Gretzky, the creator of the Evilginx phishing toolkit, tested the new method and showed how it worked perfectly with the Evilginx platform, meaning it could be adapted to steal 2FA keys during phishing attacks.

Spoofting the reverse-proxied Sec-Fetch-Dest value to "document" worked like a charm and it's beautiful

Evilginx loves it!

Kudos again to [@mrd0x](https://twitter.com/mrd0x) [pic.twitter.com/ODjblvNvho](https://pic.twitter.com/ODjblvNvho)

— Kuba Gretzky (@mrgretzky) [March 15, 2022](#)

mr.d0x told BleepingComputer that this is not a new technique and that [Zscaler reported it being used](#) by fake gaming sites in 2020 to steal Steam credentials.

Huh, looks like Steam scams are evolving. Someone tried phishing me with this really clever fake Steam login page earlier today, which mostly failed because I opened the window on my small second monitor. Watch out, everyone.

[pic.twitter.com/npGbmAqjgH](https://pic.twitter.com/npGbmAqjgH)

— TheAppleFreak (@theaaplfrack) [January 5, 2020](#)

However, now that premade templates for fake Chrome windows are available, redteamers can use them to create convincing phishing sign-in forms to test the defense of their clients or their own company's employees.

For those who wish to try out the new Browser in the Browser phishing attack, you can grab the [templates from GitHub](#).

## Related Articles:

---

[Intuit warns of QuickBooks phishing threatening to suspend accounts](#)

[New ChromeLoader malware surge threatens browsers worldwide](#)

[Screencastify Chrome extension flaws allow webcam hijacks](#)

[PDF smuggles Microsoft Word doc to drop Snake Keylogger malware](#)

[Phishing websites now use chatbots to steal your credentials](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.