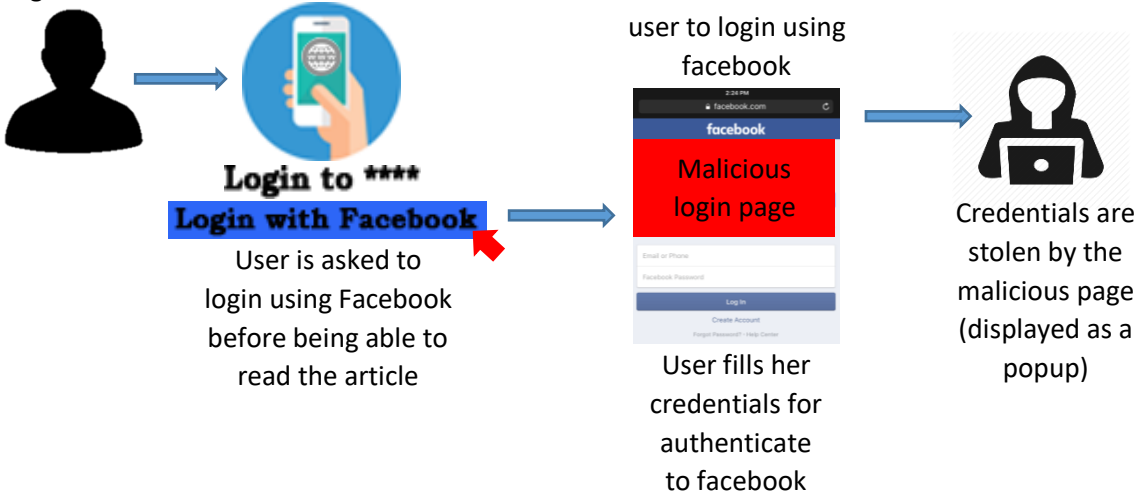
New Mobile-based 'Creative' Phishing Attack (CSB19-01)

SUMMARY

The new mobile-based 'creative' phishing attack is based on the idea that a malicious web page mimics the looks and feel of a legitimate web page to trick even the most vigilant users into giving away their login credentials to attackers. Attackers can reproduce native iOS behavior, browser URL bar and tab switching animation effects in a very realistic manner on a web-page to present fake login pages, without actually opening or redirecting users to a new tab.

HOW IT WORKS

User visits a webpage that looks legitimate



User is asked to login using Facebook before being able to read the article

Facebook login popup appears in order to allow the user to login using facebook

User fills her credentials for authenticate to facebook

Credentials are stolen by the malicious page (displayed as a popup)

MITIGATION

Use password managers that only auto-fill credentials on legit domains, helping you avoid giving away credentials to fake websites.

Enable two-factor authentication, wherever available, preventing hackers from accessing your online accounts even if they somehow manage to steal your credentials.

SECURITY RISKS

- Credentials can be stolen such as username and passwords for social media sites;
- Stealing of sensitive personal information;
- Hackers can attack your contact list by pretending to be you.