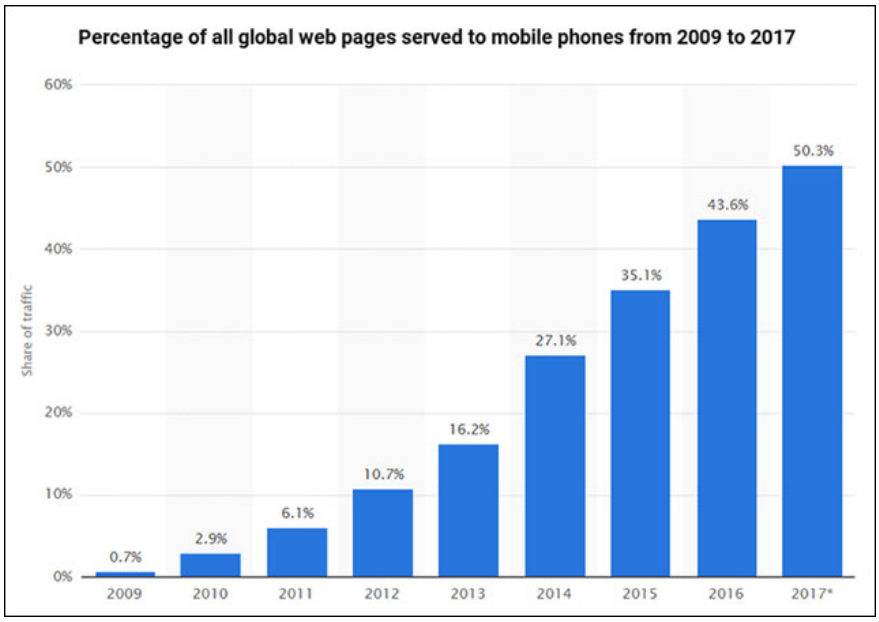
Be wary of phishing when logging on to Facebook and how to protect your Facebook account

Those who do not pay attention will easily be the victim hacked or cheated, if you regularly use Facebook, then you should start paying attention is just if you do not want to be a victim.

This is especially important if you use Facebook on a mobile device rather than a computer. Below is a graph of the percentage of websites used on mobile from 2009 to 2017 globally.



Websites worldwide have a mobile version available

Scammers are starting to exploit techniques to attack mobile users when mobile traffic is larger than PC traffic. With the fact that many mobile devices are less secure than PCs, this is a great opportunity for them.

How does Facebook login scam work?

This type of phishing uses a technique called URL padding. A regular URL will consist of three parts:

1. Domain (required)

http:/// **facebook.com** /photo.php?fbid=123456

1. Secondary domain (optional)

http:// **m** .facebook.com/ photo.php? fbid = 123456

1. Path (optional)

http://m.facebook.com/ **photo.php? fbid = 123456**

For mobile users, you will see the address m.facebook.com on your browser when using Facebook. This is to combine the domain and sub-domains displayed on the mobile version of Facebook. When you see it, you will feel safe.

URL padding is when a fraudster creates a subdomain based on a completely different domain to impersonate a page, then inserts it into a subdomain with innocuous characters to make the user think they are on the right page. real. This is an example URL from PhishLabs:

http://m.facebook.com----------validate----step1.rickytaylk.com/sign_in.html

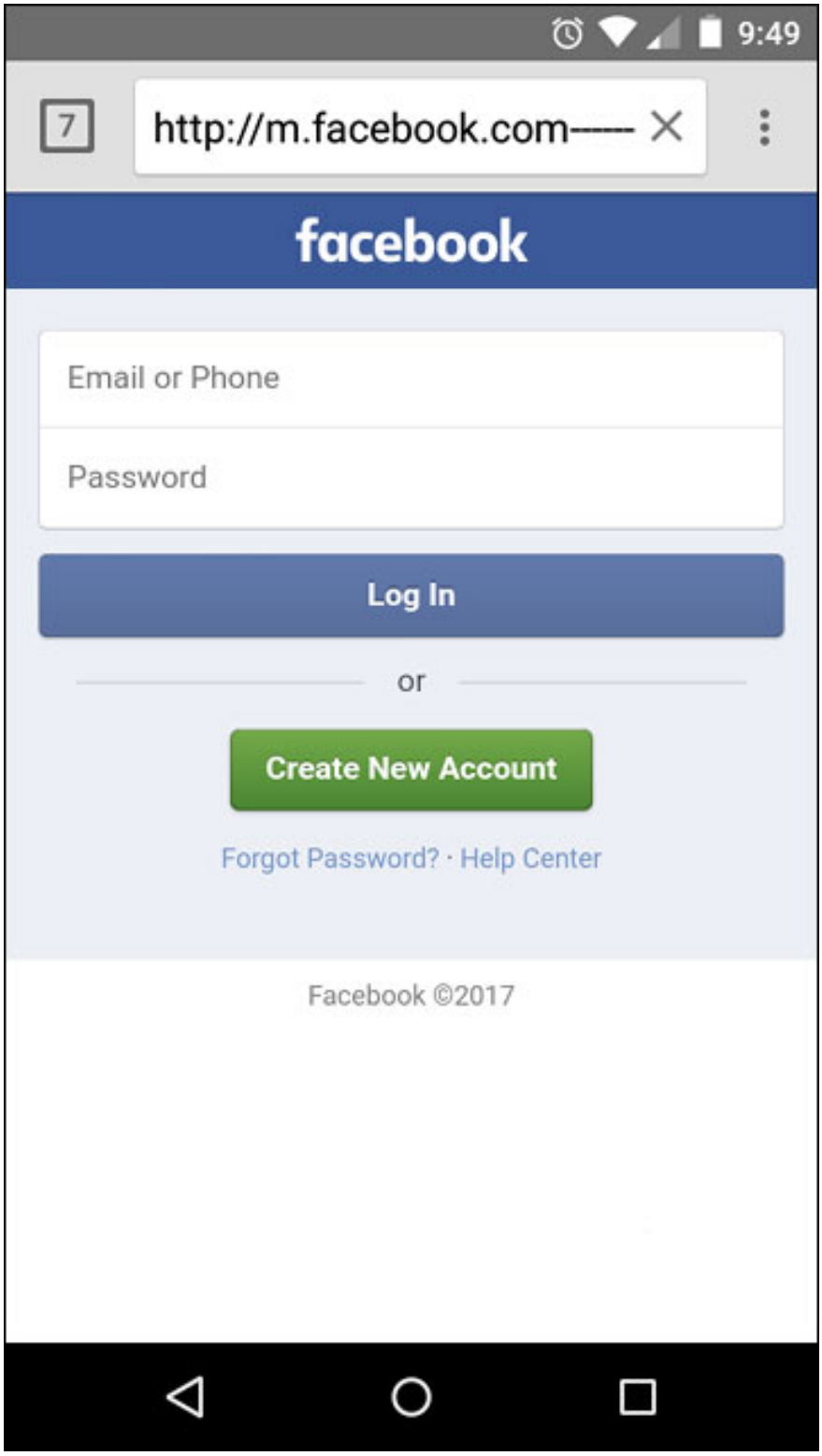
Visit this page, you will see the login screen identical to the Facebook home page on mobile, asking for login information. Users who do not pay attention will only look through the URL and see m.facebook.com and assume that it is the real page.

When finished, it is considered as done. The page will report innocuous errors (such as wrong passwords .) but your username and password information is stolen. Now an attacker can use that account to extract other accounts such as Gmail, Amazon, PayPal, banks .

Whoever pays attention will see the actual domain of this page is rickytaylk.com and it has up to 3 sub domains.

1. com ---------- validate ---- step1
2. Facebook
3. m

If you use a computer, you may notice that this URL is fake, but on the phone, the URL will only display as shown below, so it is very confusing.



The URL cannot be displayed completely on mobile browsers

This added URL can be sent in many ways such as email, instant messaging, chat applications, etc. However, the fake URL is not a new method. Earlier this year there was also an exploit discovered on Chrome (and other Chromium-based browsers), in which the URL was edited. Fortunately, the bug was patched before the scammer

could exploit it. But this also shows that completely trusting the URL is not recommended at all.

How to secure your Facebook account

You finished reading the article "**Be wary of phishing when logging on to Facebook and how to protect your Facebook account**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
