Detecting Phishing websites based on their URL attributes

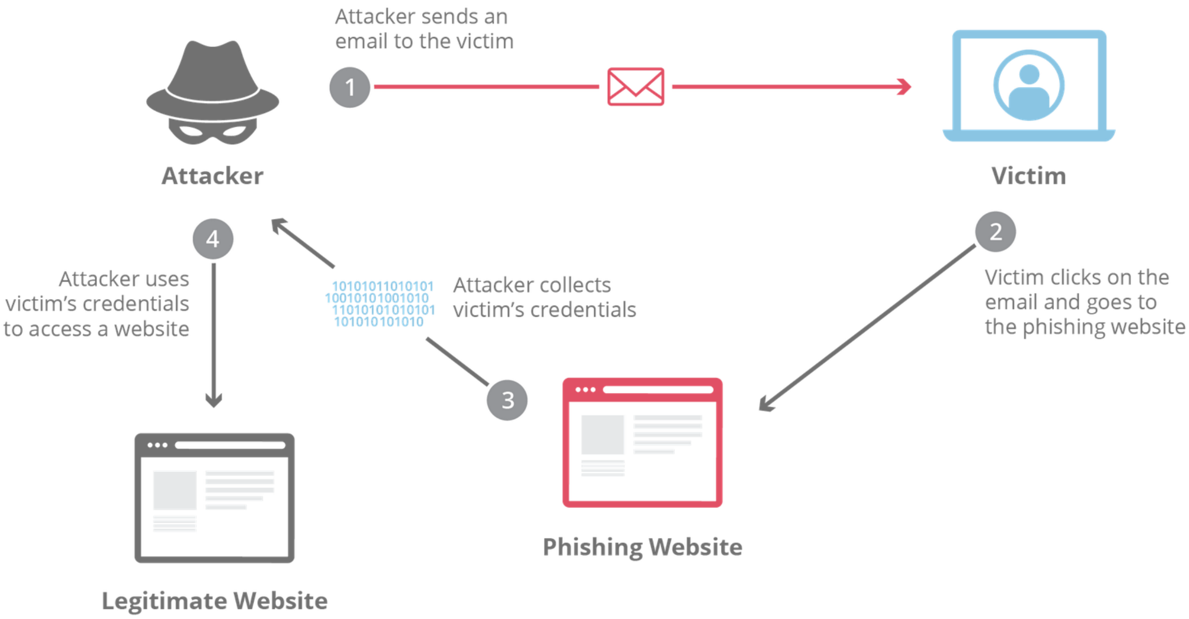
Zach Fechko

12/12/22

1 Introduction

Phishing is one of the oldest yet one of the most prevalent forms of online identity theft and fraud. And the fact that it still works to this day makes phishing is a very lucrative business for cyber criminals, and is estimated to cost businesses and individuals billions of dollars every year.

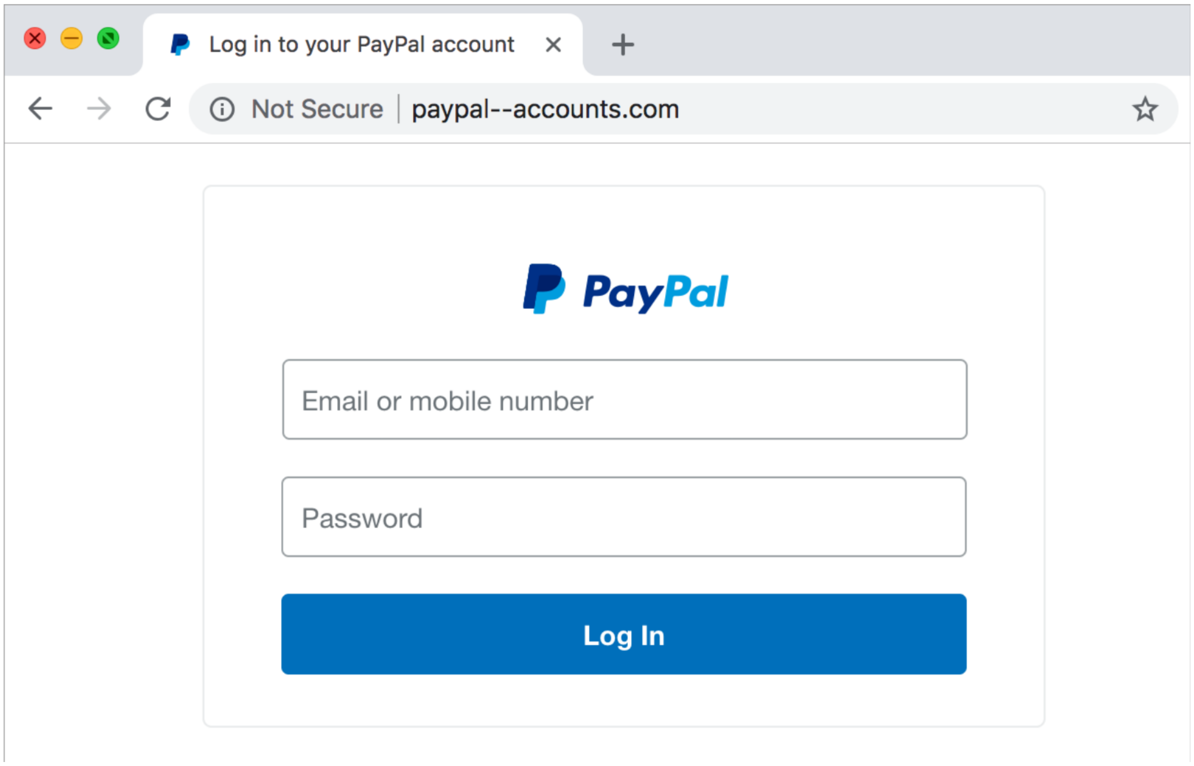
The way a phishing scam works is a cyber criminal will send an email to a user that appears to be from a legitimate source, such as their bank, PayPal, Amazon, etc. and will contain some form of urgency in order to get the victim to act on impulse and not think rationally about the email. The email will contain a link to a website, typically a login page, that will look identical to the legitimate website that they are impersonating. Once the user enters their credentials on the fake website, the cyber criminal will have access to their credentials and can do whatever they want with it.


Attacker sends an email to the victim
1
Attacker
Victim
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
2
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

:::

:::

The easiest way to tell if a website is "phishy" or not is to look at the URL of the page, oftentimes the url will be somewhat similar to the original, or not close at all in hopes that the victim doesn't even look.



:::

:::

1.1 Resources

https://www.cloudflare.com/learning/access-management/phishing-attack/