Phish Pisher

Cyber Security Final Project

Dr. Qiao

Morgan Benninghofen

Joe Ceritelli

Jeff Ross

# 

[**The Targeted Security Problem**](#_nz895u6ua0cw) **2**

[**Installation:**](#_yp8luub4dobi) **3**

[**Usage:**](#_ohn9y4hdoghw) **6**

[Enable on Google](#_4rf2rv2pffjk) 6

[Mark Subdomains](#_kkvo8f43veds) 7

[Party Mode](#_54qu0nsvi18x) 7

[Disable](#_f2quw4iy66um) 7

[Add to Whitelist](#_ofu599xtrl68) 7

[Manage Whitelist](#_opss14pjqw5w) 7

[**Testing and Examples**](#_lzh594q7uiqs) **9**

[Basic Usage](#_g2hlbj2nju28) 9

[Mark Subdomains](#_7pg5c7ov8c09) 10

[Whitelist Functionality](#_5hps5u4cduyy) 11

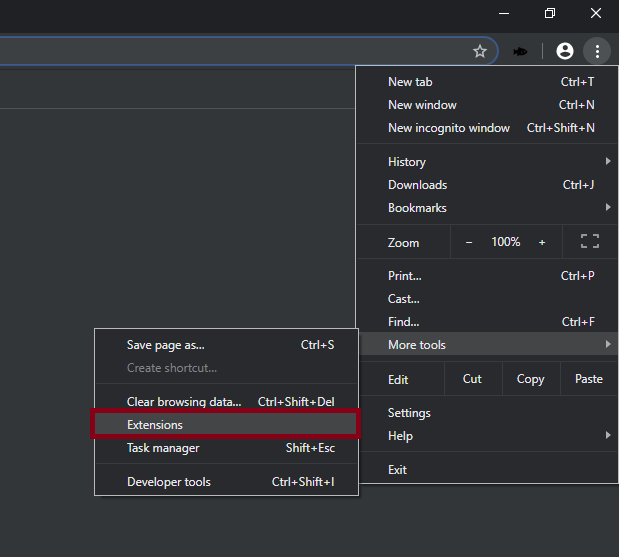
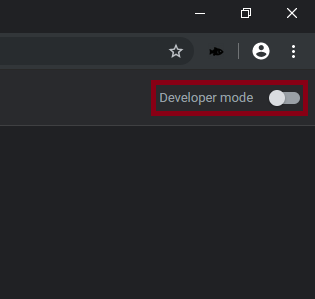
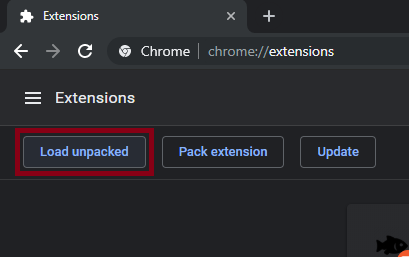
# The Targeted Security Problem

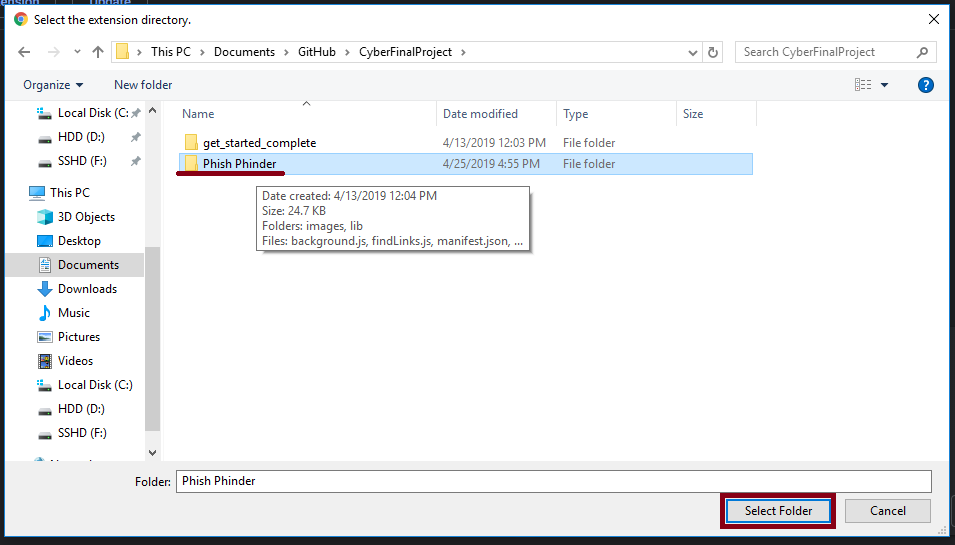
Safeguarding against phishing attacks on a website is becoming more difficult as sites become more complex and the number of links within a single page expand. Continual exposure to large sets of links on a webpage causes repetition suppression to the user. This makes it easy to modify a link within a page and take the user to an unintended location. Even if the link is not inherently malicious, it is often not the intended purpose of the user to be sent to a new domain while browsing within a site.

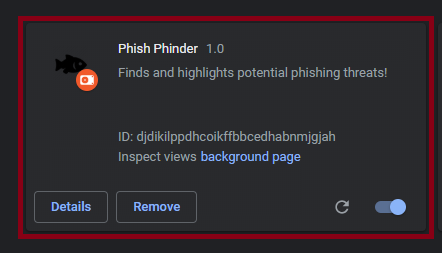
If all users were doing their due diligence, each link would be checked prior to clicking on it. This process is tedious and time consuming to the average fast paced user. The Phish Phisher intends to solve this problem by highlighting links that would move a user to an unintended domain. The plugin does not prevent the user from interacting with the page, but instead raises the awareness of the user to make more informed decisions about the links they are clicking.

# Installation:

Please note that, under normal circumstances, a the following software would normally be installed via the Chrome Web Store. But, given the size of this project, we have determined that to be outside of the scope for this project, instead this plugin can be run in developer mode using the following instructions:

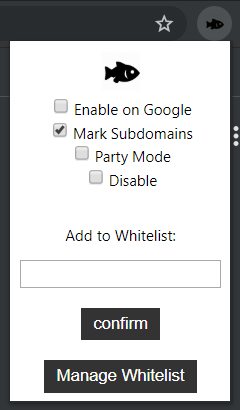
1. Turn on developer mode in Google Chrome:
   1. Go to the extensions page  
      
   2. Turn on Developer mode  
      
2. Load the extension into Chrome:
   1. Click “Load unpacked”  
      
   2. Select the Phish Phinder directory



1. The extension is now installed and can be enabled or disabled with the switch here  
   

# Usage:

The main function of this plugin is to highlight links that direct outside of the domain of the current webpage in red. However, there are added features to make the plugin more customizable. To access the options, click on the Phish Phinder icon in the top right of Google Chrome to display the following menu:



Please note that any changes made to the settings of Phish Phinder will only be applied to a page after reloading that page. Additionally, any settings changed while logged into google chrome on an account, will be applied to any computer which may be logged into that account with the extension installed.

## Enable on Google

Checking this box enables functionality on Google.com. By default this is disabled, as Google is meant to have external links, and as a result takes several seconds to load with this plugin enabled.

## Mark Subdomains

Checking this box enables the marking of subdomains. This means that if the site sdsmt.edu had a link to mcs.sdsmt.edu, it would be marked in red. By default this is enabled.

## Party Mode

Checking this box changes the way external links are highlighted. By enabling this feature, instead of marking links in red, they are marked in flashing rainbow colors. This feature is primarily to be used on sites that may have a red theme, or when links are needed to be blatantly obvious. By default this is disabled.

## Disable

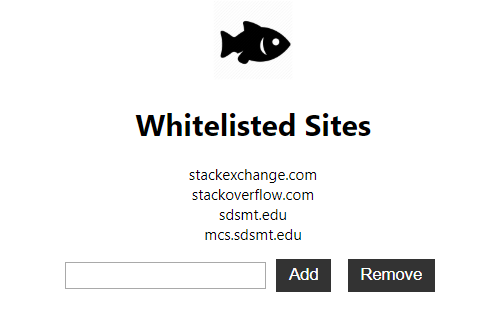
Checking this box will stop Phish Phinder from highlighting any links on any website.

## Add to Whitelist

Adding to the whitelist will ensure that any link to the site as entered to the whitelist will not be highlighted. To add to the whitelist from this page, enter the name of the site to be whitelisted in the text box. Sites are to be entered as their domain name. So for example, if you were to allow links to all pages on Amazon, you would enter “amazon.com”. Once entered, click on the confirm button to add the site to the whitelist. Please note that if the Mark Subdomain feature is enabled, it is possible to whitelist subdomains. Simply add a site with the subdomain, and the domain, in example: “mcs.sdsmt.edu”.

## Manage Whitelist

Clicking this button will refer to an options page that looks like the following:



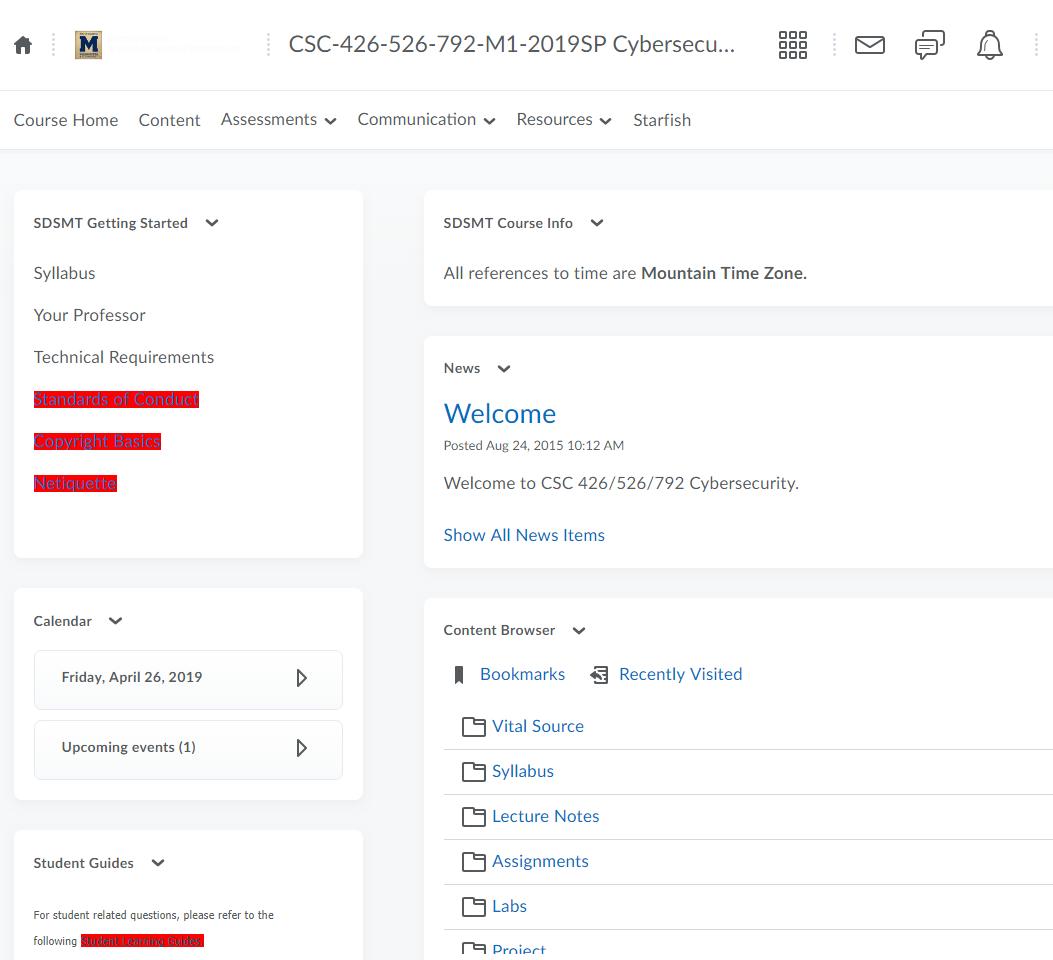
This page will show all sites currently on the whitelist, as well as the options to add and remove from the list. To add to the list, type the name of the site to be added into the textbox, and click add. More information about adding to the whitelist can be found in the “Add to Whitelist” section above. To remove from the whitelist, type the name of the site to be removed exactly as it appears on the list, and hit remove. Any site left on this list will not be highlighted as external links on the next page to be loaded.

# Testing and Examples

## Basic Usage

**Expectations**: Links within a given web page will highlighted red if they link to an outside domain. Any links that go to a page within the same domain will be unaltered.

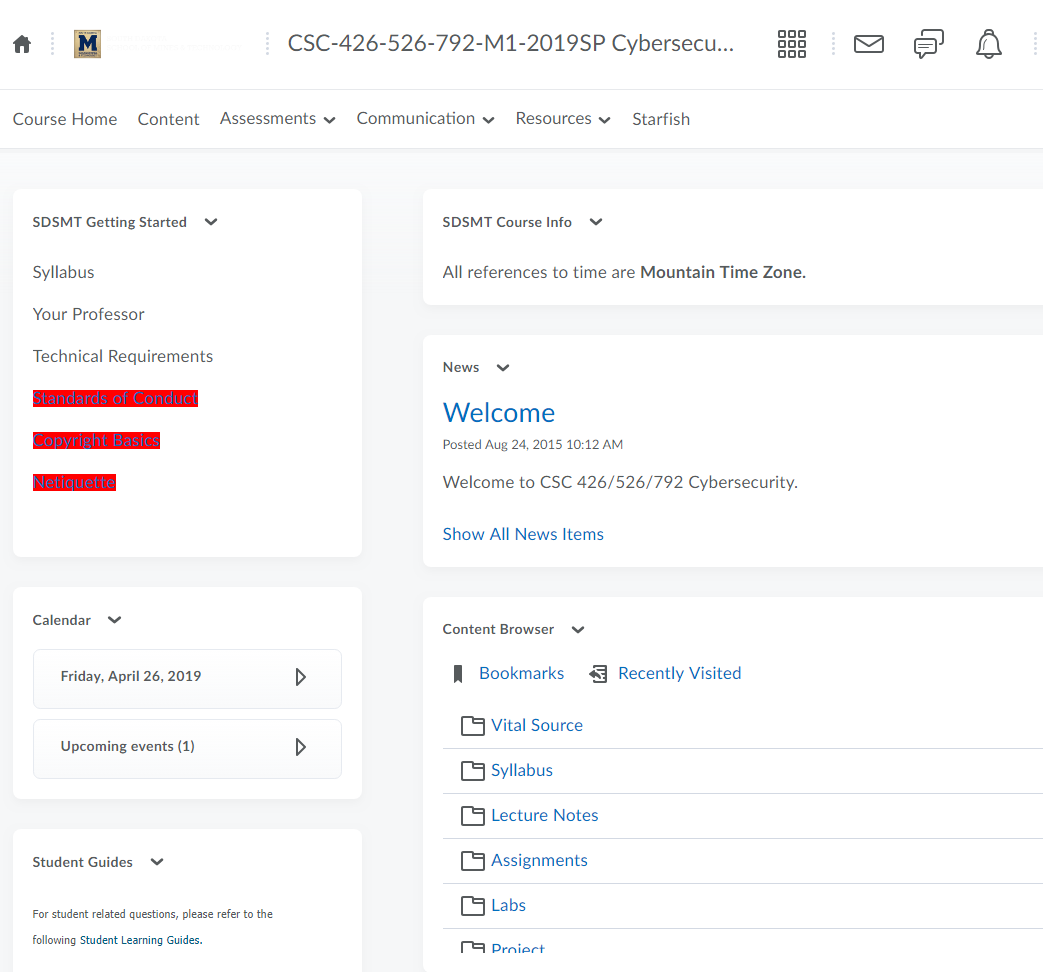
**Result**: As shown in the figure below, navigation items and content resources are unaltered. However, the Standards of Conduct, Copyright Basics, Netiquette and Student Learning Guide all link to resources outside of the domain of “d2l.sdbor.edu”. The default behavior is to treat subdomains as though they are entirely different domains.



## Mark Subdomains

**Expectations**:The Mark Subdomains feature will operate the same way as the Basic Usage, with the exception being that subdomains will not be treated as different entities as the parent domain. The default behavior is to treat subdomains as though they are entirely different domains.

**Result**: Using the same page from the Basic Usage test, we can see in the picture below that Student Learning Guide is no longer altered when the Mark Subdomains feature is disabled in the options menu.



## Whitelist Functionality

**Expectations**: A domain that has been added to the whitelist will no longer alter the links on a web page.

**Result**: “sdsmt.edu” was added to the whitelist. As shown in the picture below, Standards of Conduct is no longer being altered because it is hosted on the sdsmt.edu domain.

