

Social Engineering Project 2: Penetration Testing



Information System Security

Andrew Blyth, Jason Lee, Jun Wang, Modae Kang

2020. 04

Table of Content

1. Introduction	3
1.1 Who is CIWA?	4
1.2 Why CIWA?	4
2.Target Research and Pentest Plan	6
2.1 Email harvesting	8
2.2 Phishing	9
2.3 Researching using tools	10
2.4 Sending Phishing Email	12
2.5 Inject malware into the document	13
2.6 browser exploitation	13
3. Mitigation strategies	14
3.1 Mitigation of Phishing	14
3.2 Mitigation of browser exploitation	14
3.3 Installing Anti Virus	14
3.4 Implementing SETA	15

1. Introduction

Information security is a fast-growing discipline. The protection of information is of vital importance to organisations, corporations, governments. The development of measures to counter illegal access to information is an area that receives increasing attention. Organisations and governments have a vested interest in securing sensitive information and in maintaining the trust of clients and the people they serve. Technology on its own is not an enough safeguard against information theft. People are often the weakest link in any information security system. Even though the effectiveness of security measures to protect sensitive information is increasing, people remain susceptible to manipulation and thus the human element remains the weakest link. A social engineering attack targets this weakness by using various manipulation techniques to elicit sensitive information or to gain access to secured locations. Staff members can be influenced to divulge sensitive information, which subsequently allows unauthorised individuals access to protected systems (ScienceDirect, 2016).

Social engineering has proven to be a successful way for criminals to gain access to the targeted organizations. Once social engineers have an employee's password, they can simply log in and snoop around for sensitive data. With an access card or code in order to physically get inside a facility, the criminal can access data, steal assets or even harm people. For instance, help desk/customer service personnel are some of an organization's most vulnerable staff members since their job is to provide "help" in a friendly and polite manner. This is often exploited by an attacker to learn sensitive information. Opening an email attachment from an unknown recipient is never a good security decision. For the helpdesk/customer service representative, however, it may be a necessary part of their job in providing customer support. The attachment may be just an innocent screenshot documenting order or transaction details. However, there is the possibility that malware is lurking in the attachment, and a social engineering attack is in progress.

Security awareness training is the number one way to prevent social engineering. Employees should be aware that social engineering exists and be familiar with the most commonly used tactics. Fortunately, social engineering awareness lends itself to storytelling. And stories are much easier to understand and much more interesting

than explanations of technical flaws. But it isn't just the average employee who needs to be aware of social engineering. Senior leadership and executives are primary enterprise targets as well.

In order to fill the gaps, we decide to do a mock penetration test of one of the organizations then help them to complement their security awareness level and strengthen their weaker processes in terms of social engineering perspective. This paper illustrates how the social engineering attack scenarios are applied to verify a social engineering attack and how to mitigate the risks of a future attack.

1.1 Who is CIWA?

Calgary Immigrant Women's Association (CIWA) is a non-profit organization established in 1982 as a registered charity. CIWA is a culturally diverse settlement agency that recognizes, responds to, and focuses on the unique concerns and needs of immigrant and refugee women, girls and their families. CIWA's uniqueness is based on its gender specific mandate. Over the years, they have continually responded to emerging needs of immigrant women and girls, developed innovative programs, established meaningful partnerships, and have come to be recognized as a provincial and national leader in outcome-based gender-specific settlement services. CIWA offers programs and services that uses an integrated approach to support clients in the areas of settlement and integration, literacy and language training, employment support and bridging programs, family violence, parenting, individual counselling, in-home support, civic engagement, health, housing, and community development. All clients have access to childcare and first language support during group sessions and individual appointments. (<https://www.ciwa-online.com/about-us/who-we-are.html>)

1.2 Why CIWA?

Hackers are always on the lookout for vulnerable organizations and websites and non-profits can be the best of both worlds. Non-profit websites are generally targeted by hackers for a variety of reasons. Some of those reasons are:

1. Nonprofits are more often maintained by part-time volunteers with limited technical and IT expertise.
2. Well-maintained religious-based websites have better-than-average domain authority, credibility, and readership, which is especially appealing to black-hat SEO hackers.
3. Non-profit websites' donation forms are a potential credit card harvesting center.

Non-profit websites are usually not as well maintained, have high traffic and domain authority, and pass along credit card information. Most non-profits have less security on their website than they think they do (Jim Walker, 2019).

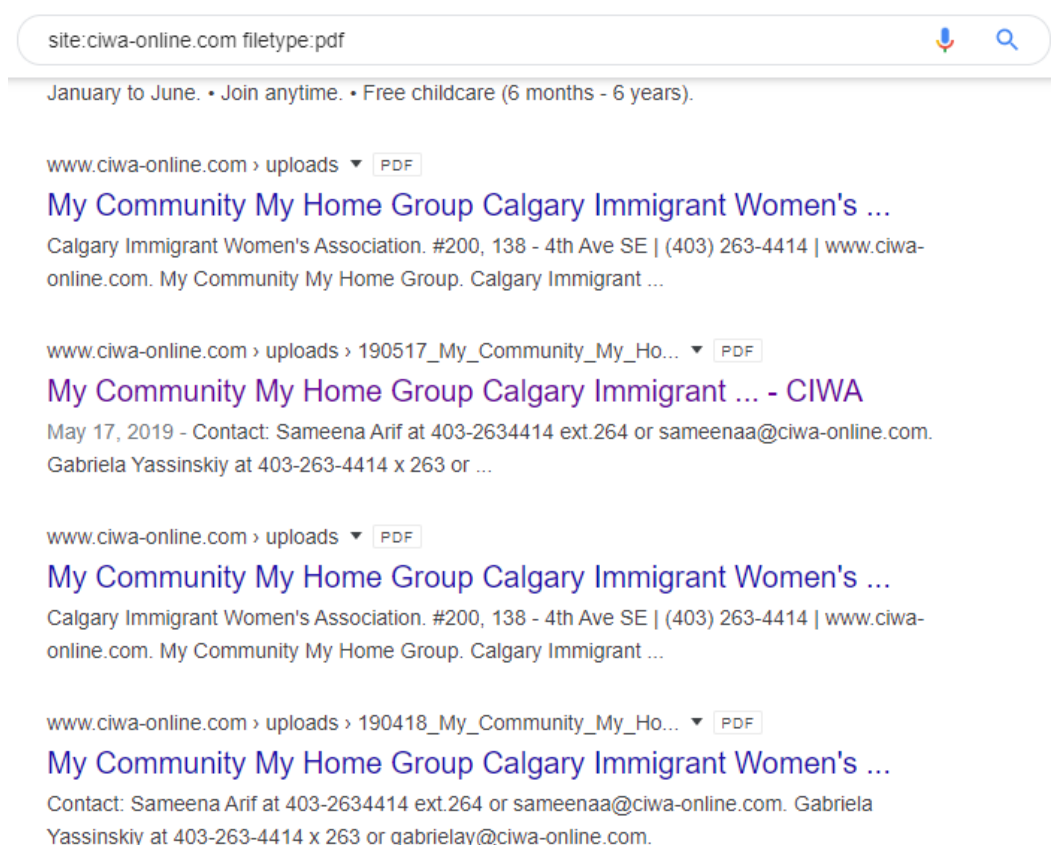
CIWA is a good example of a public funded non-profit organization. CIWA provides employment training for professionals and low to mid skilled immigrant women. Upon completion of the training, clients have the knowledge and skills to work in a Canadian workplace. The Government of Canada and Government of Alberta support them, and hundreds of companies and numerous individual donors support their business. If their business is compromised, other organizations cooperating with CIWA will be easily affected. The best way to mitigate potential cyber security risks, is starting from the weakest component, which can be a common target of social engineering.



Figure 1 Funders of CIWA (<https://www.ciwa-online.com/about-us/our-supporters.html>)

2.Target Research and Pentest Plan

Information gathering in a penetration test is the first and most important phase. Knowing your target before attacking, is a proven recipe for success. Passive information gathering is the process of collecting information about the target using publicly available information. This could include services like search engine results, whois information, background check services, and public company information. It's important to first spend some time browsing the web, looking for background information about the target organization. By doing this basic research, we can get general information such as contact information, phone numbers, emails, company structure, and so on. The google search engine is a security auditor's best friends, especially when it comes to information gathering. Google supports the use of various search operators, which allows users to narrow down and pinpoint search results.



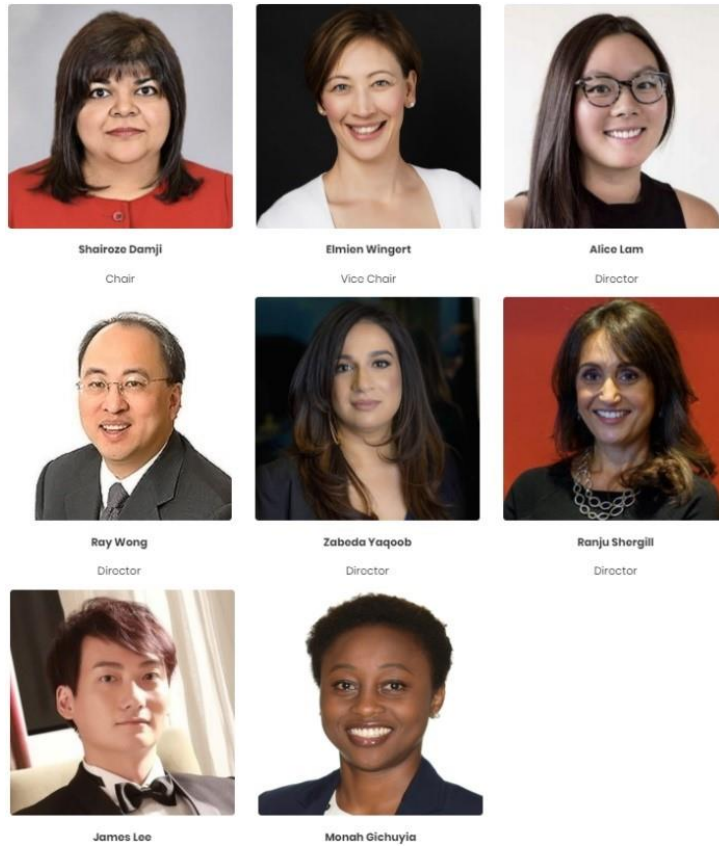


Figure 2 Board of directors (<https://www.ciwa-online.com/about-us/board-of-directors.html>)

2.1 Email harvesting

Email harvesting is an effective way of finding and organizations emails, and possibly usernames, belonging to an organization. These emails are useful in many ways, such as providing us a potential list for client-side attacks, revealing the naming convention used in the organization, or mapping out users in the organization. One of the tools is theharvester. This tool can search Google, Bing, and other sites for email addresses. We can enumerate email addresses belonging to the organization.

```
root@kali:/home/kali/Social# theHarvester -d ciwa-online.com -b google > email_google.txt
root@kali:/home/kali/Social# tail -n 25 email_google.txt
[*] No IPs found.

[*] Emails found: 17
-----
allisonm@ciwa-online.com
debrac@ciwa-online.com
director@ciwa-online.com
farzanam@ciwa-online.com
general@ciwa-online.com
jilll@ciwa-online.com
juliem@ciwa-online.com
kayleew@ciwa-online.com
language@ciwa-online.com
last@ciwa-online.com
nadiar@ciwa-online.com
raelynnp@ciwa-online.com
reception@ciwa-online.com
rekahg@ciwa-online.com
rekahg@ciwa-online.com
saraht@ciwa-online.com
tijanaj@ciwa-online.com

[*] Hosts found: 1
-----
www.ciwa-online.com:51.79.78.120
root@kali:/home/kali/Social#
```




Figure 3 Harvested email addresses

2.2 Phishing

Phishing is when a fraudulent email is made to look like a legitimate one and is sent out to gather credentials or information, and they are endemic because they work. 95% of successful cyberattacks resulted from phishing emails in 2017 (Pensar, 'Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity'). A phishing email usually looks like it comes from a trusted

organization, such as Google or Microsoft. It typically asks for the target's username and password to log onto its site, or a payment method such as a credit card number. Board members and high-level executives are prime targets for both social engineering and phishing, and techniques for both are becoming more and more sophisticated.

CIWA clearly presents lists of board of directors with name, photo and biography including previous members for the last 10 years. This executive personal information is commonly used for social engineers. We might select the appropriate executives of CIWA, then devise the scam, which usually involves a well-written email meant to exploit the trust of C-level executives who are too busy to properly vet their emails.

2.3 Researching using tools

We can also use Recon-ng as a web reconnaissance framework. Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

```
[recon-ng][default][hackertarget] > options set SOURCE ciwa-online.com
SOURCE ⇒ ciwa-online.com
[recon-ng][default][hackertarget] > run

-----
CIWA-ONLINE.COM
-----
[*] [host] ciwa-online.com (51.79.78.120)
[*] [host] rds.ciwa-online.com (206.174.195.202)
[*] [host] www.ciwa-online.com (51.79.78.120)

-----
SUMMARY
-----
[*] 3 total (3 new) hosts found.
```

Scanning the opened services to the public is one of the important factors used by social engineering techniques. We retrieved useful information related to CIWA's web server by using NMAP and Shodan.io. For example, they use Apache for web servers on 80, 443 ports and operate email servers by themselves. If there is a 3rd party technical company working closely with CIWA for system maintenance,

chances are we can manipulate technical resources in CIWA by using these contract relationships.

Ports

26	53	80	143	443	465	587	993	995	2079
2082	2083	2086	2087	2095	2096	7777			

Figure 4 Identified Opened service ports (by shodan.io)

For more in-depth investigation, we use Maltego. Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet. Maltego uses the idea of transforms to automate the process of querying different data sources. This information is then displayed on a node-based graph suited for performing link analysis.

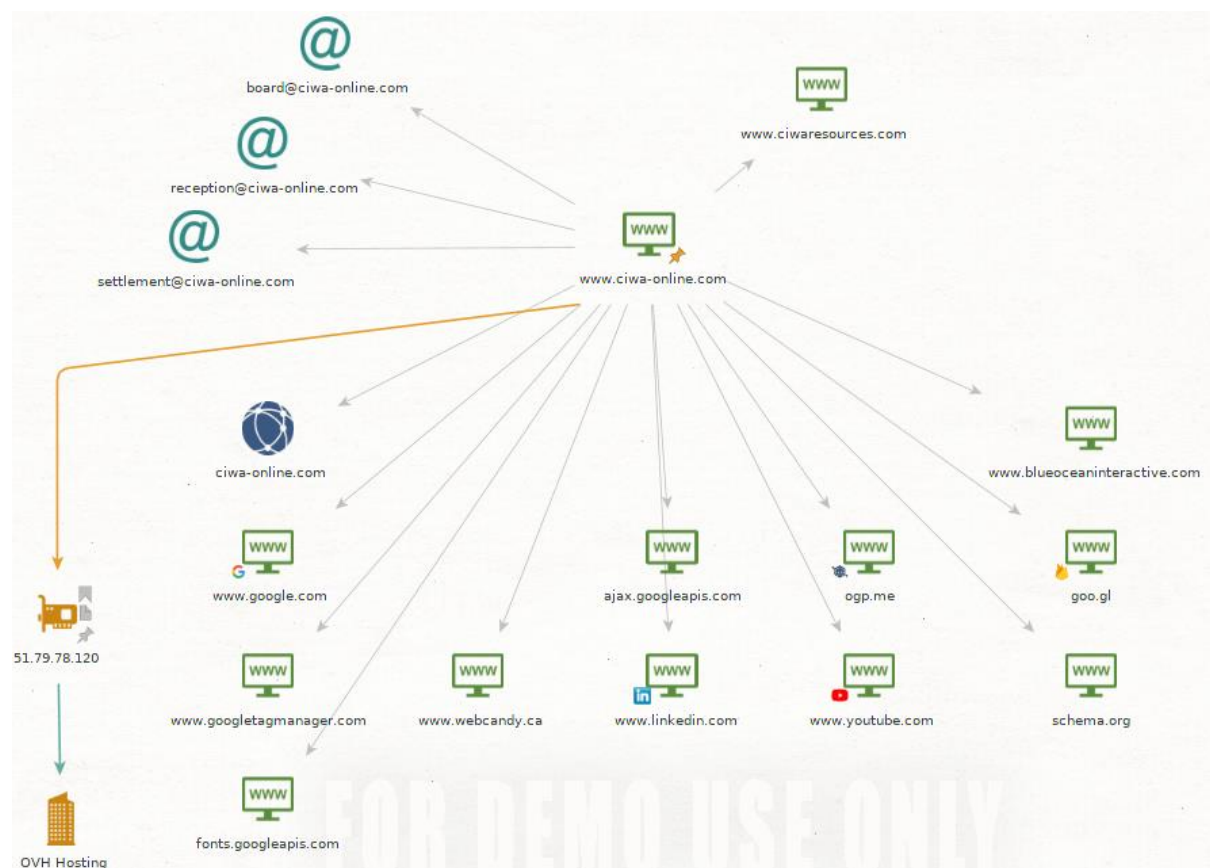


Figure 4 Acquired Information from Maltego

CIWA is operating another website ciwaresources.com and uses various external resources for providing educational services to clients, and their infrastructure was outsourced by a web hosting company called OVH Hosting.

2.4 Sending Phishing Email

As we have seen above, there is much practical information we can utilize for staging a social engineering attack. First, we may send a phishing email to CIWA to attempt to gain an internal user's credentials. CIWA is relying on their infrastructure run by a 3rd party company as they generally do not invest in infrastructure or hire skilled IT. If internal staff clicks the link, it would redirect to a fake webpage asking to change password. We can modify email sender addresses and names by using spoof email services such as Emekei's Fack Mailer.

Subject: Site Maintenance Notice

From: Monte.kang@ovh.com

Sorry for the inconvenience this morning between 4 AM to 5AM caused by our infrastructure maintenance. There was an Email server connection issue during that time, for this reason we recommend you change your email password following this instruction.

[Link]

We thank you for your understanding during.

Best regards,

Monte.Kang

2.5 Inject malware into the document

Then we can send a regular PDF document related to CIWA's current business to all of the email addresses we have acquired. CIWA has uploaded various PDFs on their website. We can guess that sharing PDF via email is a common practice. We can inject backdoor malware inside a PDF document to gain a back door into their system.

2.6 browser exploitation

BeEF is a browser exploitation framework that allows us to run several commands on Hooked browsers. Browsers can be hooked to be used in a few methods such as man in the middle attacks and access as vulnerabilities. As soon as they click on a link we will have them hooked and we will be able to run a large number of commands. These commands allow us to deliver malicious files. It allows us to show fake updates, fake logins, take screenshots, inject key loggers, and much more. Since BeEf uses Javascript, it works against all browsers including Firefox, Chrome, Internet Explorer and more.

3. Mitigation strategies

There are a variety of ways to attack the organization using information acquired from researching the target organization. As we mentioned above, we can get a lot of general information related to CIWA easily such as contact information, phone numbers, emails, company structure, and so on. Organizations need to know how to prevent and mitigate potential attacks. Here are some ways to protect organization from potential attacks.

3.1 Mitigation of Phishing

We have seen before how easy it is to send an email and pretend to be any person or any company that we want. First of all, we need to verify any suspicious emails following procedure. Looking closely at the 'from' field, verifying message source, checking the reply email, and replaying and waiting for the result. Also the education of staff about what phishing emails are and how to spot them. Also that they should report any suspected phishing emails and not feel threatened to do so. Teach them that they will not get in trouble reporting them or reporting that they clicked a suspicious link. That they can help mitigate damage by prompt reporting.

3.2 Mitigation of browser exploitation

Staff members should protect themselves from browser exploits. Most browser exploits exploit vulnerability in your browser. They will rely on some javascript code to do stuff on the browser to inject a key logger to execute code to show them fake updates and so on. The only way to protect against that is to stay up to date with the latest version of the browser. By disabling javascript execution options of browsers or installing plugins preventing javascript running, we will be able to protect ourselves from these exploits.

3.3 Installing Anti-Virus

Installing Anti-Virus software is a mandatory option. Antivirus softwares are programs that help protect your computer against most viruses, worms, Trojan horses, and other unwanted invaders that can perform malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers. Also, we should ensure both the program and the virus signature files are up to date.

3.4 Implementing SETA

One of the most important mitigate strategies is implementing SETA. It can be defined as an educational program that is designed to reduce the number of security breaches that occur through a lack of employee security awareness. A SETA program sets the security tone for the employees of an organization, especially if it is made part of the employee orientation. Awareness programs explain the employee's role in the area of Information Security. The aim of a security awareness effort is participation. Technology alone cannot solve a problem that is controlled by individuals.

Reference

ScienceDirect, 'Social engineering attack examples, templates and scenarios',
https://www.researchgate.net/publication/299344351_Social_engineering_attack_examples_templates_and_scenarios

Jim Walker(2019) Why Hackers Target Non-profit Websites And How To Defend Against It,
<https://givewp.com/cybersecurity-nonprofit-hacker-target/>

Pensar. Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity, <https://www.pensar.co.uk/blog/cybersecurity-infographic>