Airdrie, Alberta
May 13, 2017 MY FILE: 145

Ms. Suzanne Legault
The Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec
Ottawa, Ontario
K1A 1H3

Dear Ms. Legault:

Re: INCOMPLETE RESPONSE COMPLAINT- RCMP ATIP FILE: A-2017-01608

Please find attached a copy of my original ATIP request dated February 10, 2017 and the copy of RCMP's incomplete 13-page reply dated April 28, 2017. I wish to complain about the incomplete search conducted by the RCMP for the records I requested. It's almost as if they never read the wording of my original request.

I specifically requested copies of a variety of records and formats which might possibly include the information I was looking for; specifically, *"... **the number of "cyber-attacks" including the number of times hackers have attempted to access: (1) the Canadian Police Information Centre (CPIC), (2) the Canadian Firearms Registry On-line (CFRO) and (3) the Canadian Firearms Information System (CFIS) and the number of times hackers were successful in accessing information in these three computer systems and databases and/or installing viruses or malware."***

It is totally unbelievable that 25,000 Bank of Canada employees would be 'bombarded' with malware infested e-mails in just one month in November of 2015 and these three major databases (CPIC, CFRO and CFIS) controlled by the RCMP had only these two 'Clickjacking' incidents.
http://business.financialpost.com/fp-tech-desk/hackers-bombard-the-bank-of-canada-with-cyberattacks?__lsa=f998-c75c

Similarly, it is impossible to believe that the RCMP Commissioner, his Executive Committee and senior officers responsible for the security of these three major databases would not have received reports, presentations, etc, etc. about the number of 'cyber-attacks' these three major databases had received. The very least they should have received is reports on how these systems are so incredibly secure from cyber-attacks that they no one even tries to get into them while every other database in the world is dealing with thwarting these attacks. See the attached links to recent articles in the news.

In 2011, I received the attached statistics from the RCMP documenting 480 'Investigated and Founded' breaches of CPIC between 1995 and 2010. And these breaches were committed by police employees trusted with access to and the security of the CPIC database. Now the RCMP would have us believe that only two attempts have ever been made to access these three systems CPIC, CFRO and CFIS by unscrupulous people trying to infiltrate these databases? It makes no sense. http://dennisryoung.ca/wp-content/uploads/2017/05/CPIC-Breaches-1995-2010.pdf

In closing I leave you with the following quote I transcribed from the Global National television news broadcast last night. **BILL THOLL, PRESIDENT & CEO, HEALTHCARECAN, GLOBAL NATIONAL TV NEWS - MAY 12, 2017:** "The experts will tell you, there are only two types of hospitals thems that have been hacked and thems that don't know." http://globalnews.ca/news/1148831/watch-global-national/

Thanks for your help to find the records I requested.

Yours sincerely,

[Original signed by]

Dennis R. Young
1330 Ravenswood Drive SE
AIRDRIE, AB T4A 0P8
Home Phone: 587-360-1111
New E-Mail: dennisryoung@telus.net
Website: www.dennisryoung.ca

NATIONS RESPOND TO BIGGEST EXTORTION CYBERATTACK EVER RECORDED, NEW ATTACKS FEARED
The cyber assault has infected tens of thousands of computers in nearly 100 countries, with Britain's health system suffering the worst disruptions.
By Jeremy Wagstaff and Eric Auchard Reuters - May 13, 2017
http://globalnews.ca/news/3448980/biggest-extortion-cyberattack-ever-recorded-hits-dozens-of-countries/

CANADIAN AGENCY BREACHED AS HACKERS EXPLOIT NEW SOFTWARE BUG
Statistics Canada, which said it stopped the intrusion before hackers stole any data, is the first high-profile organization to say it was hacked due to a new security bug in software known as Apache Struts 2. The software is commonly used in websites of governments, banks, retailers and other large organizations. By Reuters - March 13, 2017
http://www.thefiscaltimes.com/latestnews/2017/03/13/

BILL THOLL, PRESIDENT & CEO, HEALTHCARECAN - GLOBAL NATIONAL TV NEWS - MAY 12, 2017
"The experts will tell you, there are only two types of hospitals thems that have been hacked and thems that don't know." http://globalnews.ca/news/1148831/watch-global-national/

PUBLIC SAFETY CANADA: CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)
https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Your file / Votre référence
GA-1516-3-01608/17

Our file / Notre référence
A-2017-01608

APR 2 8 2017

Received May 9, 2017

Mr. Dennis R. YOUNG
1330 Ravenswood Drive South East
Airdrie, Alberta T4A 0P8

Dear Mr. YOUNG:

This is in response to your request under the *Access to Information Act*, which was received by this office on February 10, 2017, to obtain:

> *For the period from January 1, 2015 to present, please provide copies of records, documents, studies, reports, presentations, spreadsheets, briefings, communications, correspondence showing the number of cyber attacks including the number of times hackers have attempted to access: (1) the Canadian Police Information Centre (CPIC), (2) the Canadian Firearms Registry On-line (CFRO) and (3) the Canadian Firearms Information System (CFIS) and the number of times hackers were successful in accessing information in these three computer systems and databases and/or installing viruses or malware*

Enclosed is a copy of all the information to which you are entitled. Please note that some of the information has been exempted pursuant to sections 16(2), 19(1) of the *Act*, a description of which can be found at: http://laws-lois.justice.gc.ca/eng/acts/A-1.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days after the day that you become aware that grounds for a complaint exist. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

> Office of the Information Commissioner of Canada
> 30 Victoria Street, 7th Floor
> Gatineau, Quebec K1A 1H3

Should you wish to discuss this matter further, you may contact Ms. Crystal Holub at Crystal.Holub@rcmp-grc.gc.ca . Please quote the file number appearing on this letter.

Regards,

S/Sgt Kent Sun

Insp. Richard Haye
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

Canada

ATIPB - Re: Possible Clickjacking

From: DSB_ITS
To: Mace, Ryan
Date: 2016/06/22 8:25 AM
Subject: Re: Possible Clickjacking

Hi Ryan,

We are looking into it.

Thanks
Mary

Mary Wiaz
IT Security Analyst
Information Technology Security
Departmental Security Branch
HQ Leikin, Ottawa
613-843-5977
mary.wiaz@rcmp-grc.gc.ca

>>> On 2016/06/21 at 3:49 PM, in message <57699A5F.47B : 170 : 17821>, Ryan Mace wrote:

> Good day,
>
> On June 20, 2016 it was brought to the attention of CAO
> Clickjacking
> (https://en.wikipedia.org/wiki/Clickjacking).
>
> *"Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.[1][2][3][4] It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.[5]"* - Wikipedia
>
> Possible resolutions include
>
> I have attached 2 files.
> and the other to illustrate how www.google.ca (google-clickjack.html) has defended against this
>
> Please keep us informed.

Ryan Mace
Corporate Architecture Office
Royal Canadian Mounted Police
(613) 993-0874
ryan.mace@rcmp-grc.gc.ca

ATIPB - Fwd: Possible Clickjacking

From: Brenda Deugo
To: Leblanc, Marc
Date: 2016/06/22 9:56 AM
Subject: Fwd: Possible Clickjacking
CC: Cote, Sylvie; Mace, Ryan; Myelde, Kirk; Olivieri, Dario
Attachments: Re: FW: follow-up To CAFC feedback; Possible Clickjacking

Marc,

Can you looking into this please. From the attached it was sent to the DSB_ITS mailbox yesterday.

Brenda

>>>

From: Kirk Myelde
To: Boudreau, Paul; Deugo, Brenda
Date: 2016/06/22 9:38 AM
Subject: Fwd: Possible Clickjacking

Brenda/Paul

Just got this now have you see it. Your guys have it but wanted to make sure you were aware since the RCMP is being mentioned online.

Kirk

>>> Ryan Mace 6/22/2016 9:31 AM >>>
Kirk,

As requested, attached is:

1) the initial email received from the public individual
2) the email that was sent to DSB_ITS informing them of the issue after I researched the topic.

Also,

If you need anything more please let me know,

Ryan Mace
Corporate Architecture Office
Royal Canadian Mounted Police
(613) 993-0874
ryan.mace@rcmp-grc.gc.ca

ATIPB - Re: FW: follow-up To CAFC feedback

From: Cynthia Shea
To: Anderson, Stephen; Mace, Ryan
Date: 2016/06/20 7:12 AM
Subject: Re: FW: follow-up To CAFC feedback

Ryan,

Do you have any thoughts on this?

Stephen - I am adding you as you are now the new IPE 2.0 lead.

Cindy

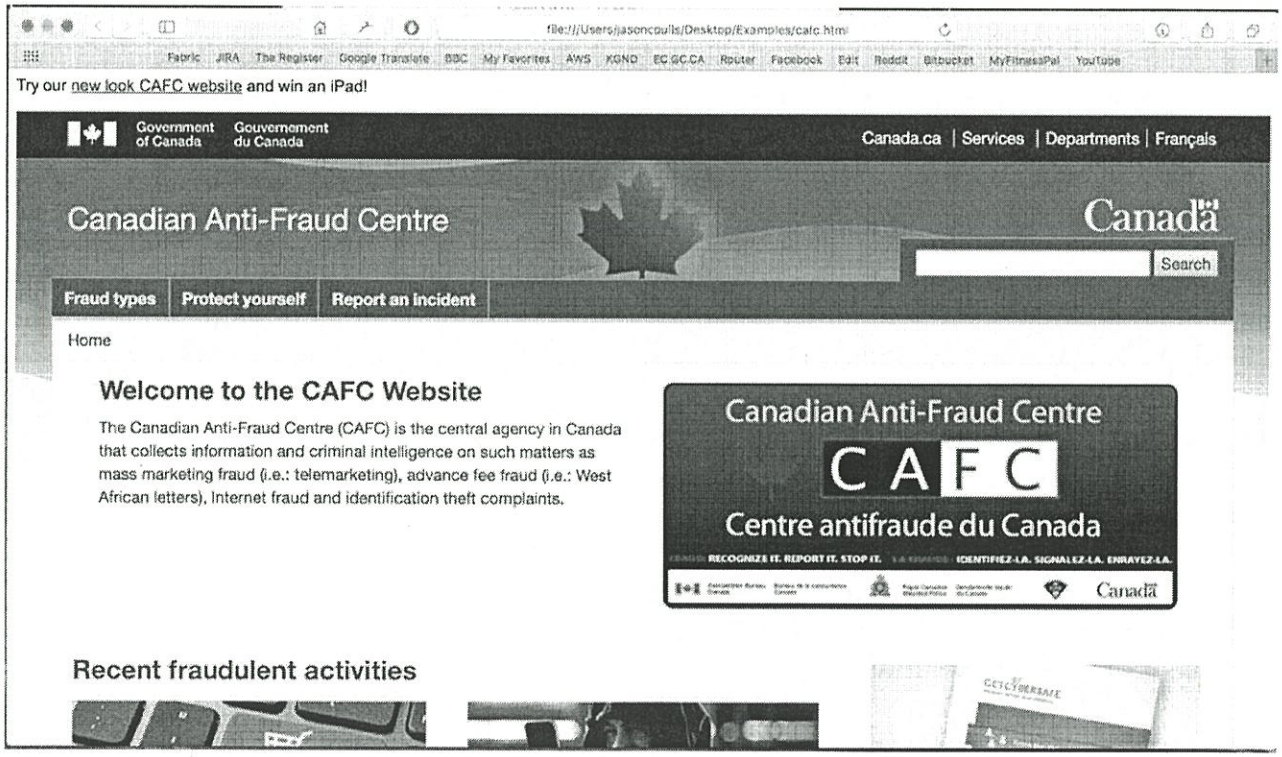
>>> "Jeff Thomson" <jthomson@antifraudcentre.ca> 17/06/2016 8:54 AM >>>

From:
Sent: June-16-16 10:24 AM
To: Jeff Thomson <jthomson@antifraudcentre.ca>
Subject: Re: follow-up To CAFC feedback

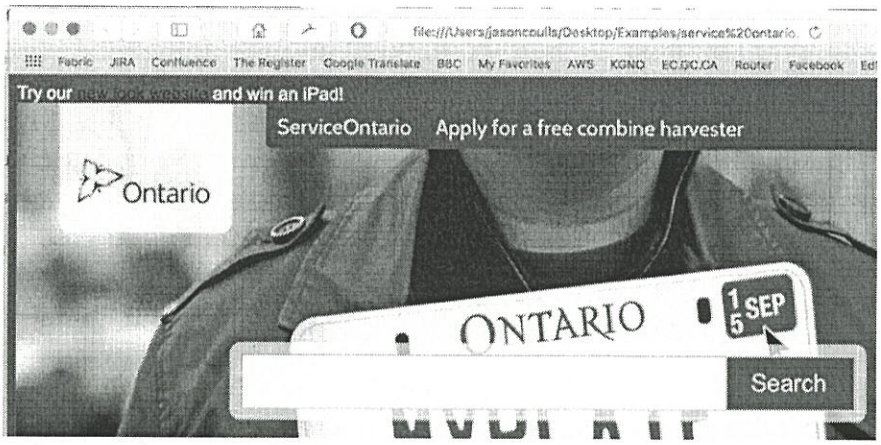
Hi Jeff,

Absolutely…

Here's a screenshot showing (top left corner shows the issue).



The original issue I was going to point out before finding the issue with the CAFC site



There's an irony in that when I was going to report the original issue, I found the CAFC system suffered the same.

Now, whilst all that is a problem, there's a really massive issue undermining anything you fix (which going back up the chain of issues was the very first item I was going to raise before the CAFC); Assuming you (or another government dept) fix your own systems up

In short, it's a total mess and I'm trying to do what I believe is the right thing in raising the alarm, but couldn't even upload a screenshot through the CAFC system.

As for calling,

Cheers

On Jun 16, 2016, at 10:07 AM, Jeff Thomson <jthomson@antifraudcentre.ca> wrote:

Hi Jason,

Thanks very much for the feedback, I would like to discuss further is there a number you can be reached at?

Thanks again, Jeff

Jeff Thomson
Operational Support Unit / Unité de soutien opérationnel
Canadian Anti-Fraud Centre / Le centre antifraude du Canada
Royal Canadian Mounted police / Gendarmerie royale du Canada
Dir/Tl:(705) 494-3630 Fax/Tlc (705) 494-4755
Fraud...Recognize It...Reject It...Report It

ATIPB - Possible Clickjacking

From: Ryan Mace
To: DSB_ITS
Date: 2016/06/21 3:49 PM
Subject: Possible Clickjacking
CC: Thomas, Michael
Attachments: google-clickjack.html; rcmp-clickjack.html

Good day,

On June 20, 2016 it was brought to the attention of CAO
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking).

"Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.[1][2][3][4] It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.[5]" - Wikipedia

Possible resolutions

I have attached 2 files.
to illustrate how www.google.ca (google-clickjack.html) has defended against this

Please keep us informed.

Ryan Mace
Corporate Architecture Office
Royal Canadian Mounted Police
(613) 993-0874
ryan.mace@rcmp-grc.gc.ca

ATIPB - RE: Possible clickjacking

From: "Mcevoy, John (SSC/SPC)" <john.mcevoy@canada.ca>
To: Ryan Mace <Ryan.Mace@rcmp-grc.gc.ca>
Date: 2016/06/22 12:22 PM
Subject: RE: Possible clickjacking
CC: Kirk Myelde <Kirk.Myelde@rcmp-grc.gc.ca>, Michael Thomas <Michael.Thomas...

Hi Ryan,

Thank you for the email and I have copied our Technical Lead (Louis Leduc) on my response so that he is aware of the situation. We plan on talking to our contacts and get their perspective on the situation. Hopefully we can speak with them this afternoon and then have a discussion with RCMP after that. Would that work for you? I could set-up a call for tomorrow morning if we can talk with this afternoon.

Thanks,

John

From: Ryan Mace [mailto:Ryan.Mace@rcmp-grc.gc.ca]
Sent: June-22-16 12:00 PM
To: Mcevoy, John (SSC/SPC)
Cc: Kirk Myelde; Michael Thomas
Subject: Possible clickjacking

John,

I was given your name by Jeremy Arndt here at the RCMP.

On June 20, 2016 it was brought to our attention that
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking).

"Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a

Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.[1][2][3][4] It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.[5]" - Wikipedia

There are several ways to prevent/defend against Clickjacking

I was hoping to discuss further over the phone.

Ryan Mace
Corporate Architecture Office
Royal Canadian Mounted Police
(613) 993-0874
ryan.mace@rcmp-grc.gc.ca

ATIPB - Clickjacking

From: Jeremy Arndt
To:
Date: 2016/06/22 2:23 PM
Subject: Clickjacking
CC: Leblanc, Marc; Mace, Ryan
Attachments: FW: Possible clickjacking

We are already taking steps internally in our department awareness, confirmation, and further distribution.

Sharing with you for

Jeremy Arndt
Senior Analyst - CFP Applications
Systems Delivery and Support, IM/IT Program
Royal Canadian Mounted Police
613-993-3604 | Jeremy.Arndt@rcmp-grc.gc.ca

ATIPB - FW: Possible clickjacking

From: "Mcevoy, John (SSC/SPC)" <john.mcevoy@canada.ca>
To: "Jeremy.Arndt@rcmp-grc.gc.ca" <Jeremy.Arndt@rcmp-grc.gc.ca>
Date: 2016/06/22 1:28 PM
Subject: FW: Possible clickjacking

Hi Jeremy,

I hope all is well. I just wanted to make sure you were aware of this email. Can you give me a call.

Thks,

John

From: Ryan Mace [mailto:Ryan.Mace@rcmp-grc.gc.ca]
Sent: June-22-16 12:00 PM
To: Mcevoy, John (SSC/SPC)
Cc: Kirk Myelde; Michael Thomas
Subject: Possible clickjacking

John,

I was given your name by Jeremy Arndt here at the RCMP.

On June 20, 2016 it was brought to our attention that
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking).

"Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.[1][2][3][4] It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.[5]" - Wikipedia

There are several ways to prevent/defend against Clickjacking

I was hoping to discuss further over the phone.

Ryan Mace
Corporate Architecture Office
Royal Canadian Mounted Police
(613) 993-0874
ryan.mace@rcmp-grc.gc.ca

ATIPB - Re: Possible clickjacking

From: Chris Power
To: Mace, Ryan
Date: 2016/06/23 9:19 AM
Subject: Re: Possible clickjacking
CC: Gordon, Jeff; Myelde, Kirk; Thomas, Michael

Hi Ryan:

Thanks for the heads up. The guys on our tech team are aware
we'll review the article and go from there.

Cheers

C

>>> Ryan Mace 2016/06/22 12:06 PM >>>
John,

On June 20, 2016 it was brought to our attention that
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking).

"Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.[1][2][3][4] It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.[5]" - Wikipedia

There are several ways to prevent/defend against Clickjacking

I was hoping to discuss further over the phone.

Ryan Mace
Corporate Architecture Office
Royal Canadian Mounted Police
(613) 993-0874
ryan.mace@rcmp-grc.gc.ca

ACCESS TO INFORMATION ACT

Access to Information Request Form

For official use only:

My File: 145

Federal Government Institution:

RCMP HQ OTTAWA & CANADIAN FIREARMS PROGRAM

Details regarding the information being sought:

Reference is being made to this article in the FINANCIAL POST - HACKERS ARE BOMBARDING THE BANK OF CANADA WITH CYBER ATTACKS AND THE CRACK IN THE BANK'S ARMOUR IS ITS EMPLOYEES - Employees at the Bank of Canada in November 2015 were bombarded with 25,000 similar, innocuous-looking emails carrying malware designed to steal banking credentials. By Claire Brownell - Last Updated: Jan 27, 2017, 11:21 AM ET
http://business.financialpost.com/fp-tech-desk/hackers-bombard-the-bank-of-canada-with-cyberattacks?__lsa=f998-c75c

For the period from January 1, 2015 to present, please provide copies of records, documents, studies, reports, presentations, spreadsheets, briefings, communications, correspondence showing the number of "cyber attacks" including the number of times hackers have attempted to access: (1) the Canadian Police Information Centre (CPIC), (2) the Canadian Firearms Registry On-line (CFRO) and (3) the Canadian Firearms Information System (CFIS) and the number of times hackers were successful in accessing information in these three computer systems and databases and/or installing viruses or malware.

Method of access preferred: ❑ Receive copies of originals ❑ Examine originals in government offices

Name of Applicant: **Dennis R. Young**
Address: **1330 Ravenswood Drive SE**
Airdrie, Alberta T4A 0P8

Telephone Number: 587-360-1111 **E-Mail:** dennisryoung@telus.net

This request for access to information under the Access to Information Act is being made by:

❑ **a Canadian citizen, permanent resident or another individual present in Canada, or**

❑ **a corporation present in Canada**

Cheque # 530

[Original signed by]

Signature: _____ **Date: February 10, 2017**

Dennis R. Young