



RANSOMWARE

'CYBER-SMART'

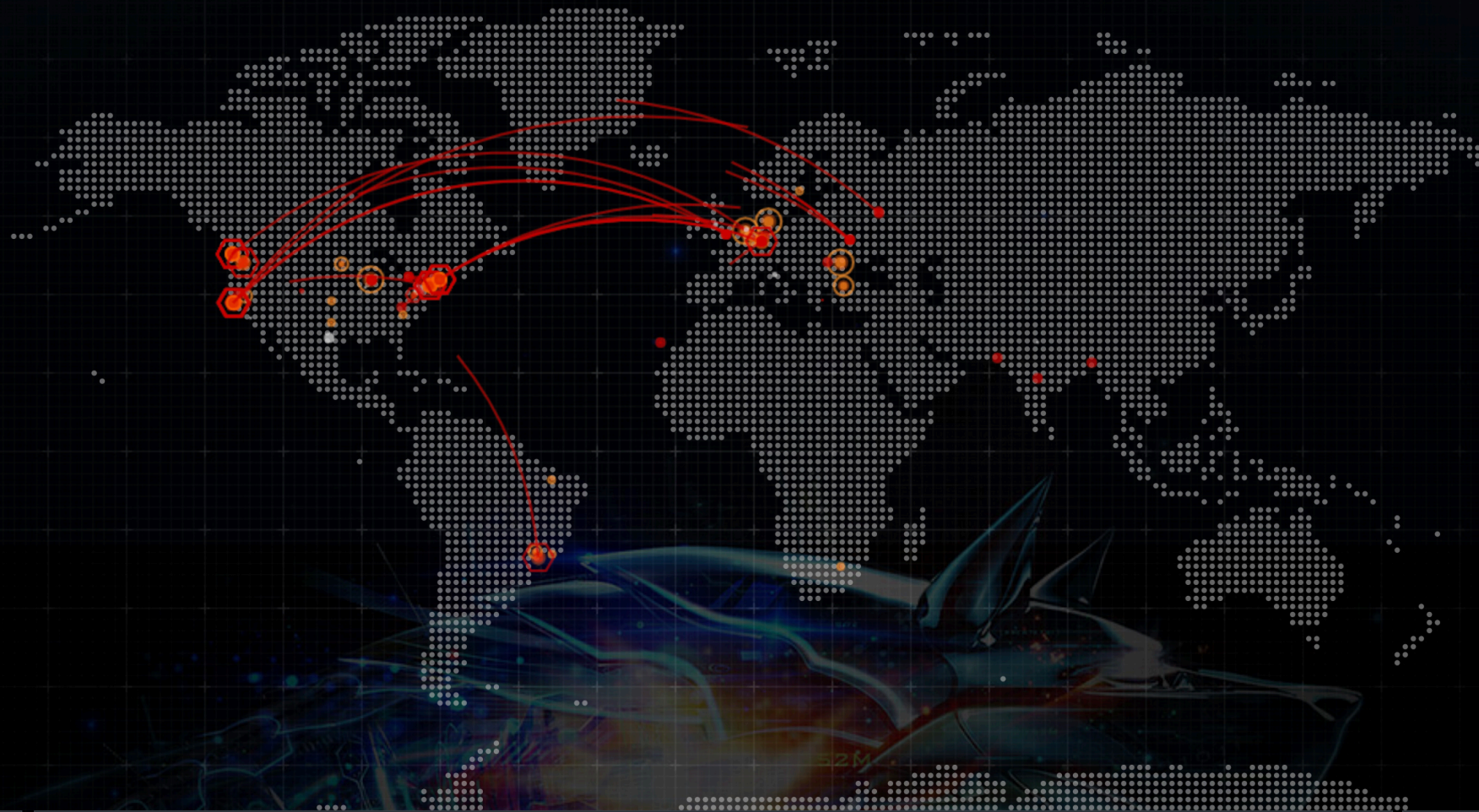
Safeguard your newspaper against ransomware attacks

- ▶ In 2019 there were over 4,600 reported ransomware attacks in Canada. The cost associated with these attacks is an estimated \$2.3 billion
- ▶ Cybercrime costs the global economy in excess of \$400 billion each year
- ▶ Over 18 million known viruses exist

Source: Emsisoft

IT CAN'T HAPPEN TO US

THINK AGAIN



LEGEND

- ATTACKS
- INFECTIONS
- SPAM

LIVE ATTACKS

TIME	ATTACK	ATTACK TYPE	ATTACK COUNTRY	TARGET COUNTRY
TUE 3 NOV 9:38:30 AM	N/A	ATTACK	UNITED STATES	UNITED STATES
TUE 3 NOV 9:38:30 AM	N/A	ATTACK	SPAIN	GERMANY
TUE 3 NOV 9:38:31 AM	?DBINSTALLER.EXE:0000F00...	INFECTION	UNITED STATES	N/A
TUE 3 NOV 9:38:29 AM	N/A	SPAM	RUSSIA	N/A
TUE 3 NOV 9:38:29 AM	?ASSISTANT_INSTALLER.EXE...	INFECTION	PERU	N/A
TUE 3 NOV 9:38:35 AM	N/A	ATTACK	UNITED STATES	UNITED STATES
TUE 3 NOV 9:38:32 AM	N/A	ATTACK	UNITED STATES	UNITED STATES

LOCATIONS

- UNITED STATES
- GERMANY
- UNITED KINGDOM
- FRANCE
- CANADA
- BRAZIL
- RUSSIA
- INDIA
- TURKEY

[HTTPS://THREATMAP.BITDEFENDER.COM/](https://threatmap.bitdefender.com/)



WHAT IS MALWARE?

Malware is an abbreviated term meaning **Malicious Software** that refers to a variety of hostile or intrusive software.

- viruses • worms • trojans • spyware • adware
- scareware • **ransomware**

RANSOMWARE

Ransomware is malicious software that removes the users' ability to access their computer. Ransomware can come from links in email, attachments, malicious codes on websites or messaging service. To restore the system the criminal demands payment with the promise that all will be well.

NEVER PAY THE RANSOM!

From my experience with thousands of cases you seldom will have your files restored as promised. Most often the criminals simply do not have the ability to actually restore them.

Ransomware scripts are purchased from coders who sell the creations to the highest bidder. This is not to say that you will never have the files restored if you pay, but why take the chance.

Preparing your business for what is surely to happen makes more sense, both in security and peace of mind. Take steps to mitigate disaster before it happens.



SIMPLE STEPS TO MITIGATE DAMAGE

Approach your security with an **ONION** in mind: multiple layers of security protecting the core.

Employ a minimum of three backup redundancies.

1. Enable your OS backup system. i.e. Time Machine, Windows backup
2. Keep current working backups of your important files and databases off-site on a secure server (*hosted in Canada preferably*).
3. Maintain a daily backup of files on an external HDD that is **NOT** connected to a computer or internet after it is used for the backup.

When ransomware attacks a computer the first thing it looks to do is take out or infect your backups. Maintaining three backups will ensure that you are up and running in a matter of hours.

SIMPLE STEPS TO MITIGATE DAMAGE

- ▶ Always ensure your OS is up-to-date with the latest available version. **Never turn off Windows or Mac updates!**
- ▶ **Run anti-virus software** on every device connected to your office network. While you should never run two antivirus programs together you can run a combination of your antivirus software and Malwarebytes for added security.
- ▶ **Never allow** external non-office devices on your network. It is the digital equivalent to sleeping around. You never know where that device was or what malicious programs it carries.
- ▶ Run an office router system with advanced security features. I recommend Eero. Eero provides numerous advanced security features, blocking suspicious domains, botnets and phishing sites. It allows for a guest account on a separate network isolated from your main network.

SIMPLE STEPS TO MITIGATE DAMAGE

- ▶ **Never open an email or web link that you were not expecting.** This can be hard in an office environment with the continuous flow of information to your inbox, however, extreme caution should always be exercised with links and archived file attachments i.e. zip, rar, google doc links etc.
- ▶ **Train, Train, Train** - No matter what you employ as in-house security measures, your business and network is only as strong as the person sitting behind the computer. Training is paramount in stopping malicious software from entering your network.
- ▶ Keep up-to-date on the latest ransomware trends. Holding monthly office meetings and email/web browsing security refreshers is a must. Sending out fake phishing emails to your employees is also an option to test your preparedness.
- ▶ Adopt safe browsing practices for your office, laying out what type of website is acceptable and what is not.

EMAIL – SPOTTING THE FAKE

- ▶ Do not open emails from an unknown source.
- ▶ Do not open emails with dubious subject lines such as “You have won”, “We require more information”, “Attn: Invoice attached”, etc.
- ▶ Use a commonsense approach to email. Pay-pal, eBay and CRA to name a few, will never ask you to click a link and update your information.
- ▶ Identify the email address that the email was sent from, look for inconsistencies such as spelling mistakes, bad spaces and misspelt corporate names.
- ▶ Ensure your email client is set to text only or basic html.
- ▶ Ensure MS Office (Word and Excel) has macros disabled.

EMAIL - SPOTTING THE FAKE

The screenshot shows an email client window with the following details:

- Search:** All, Inbox (6), VIPs, Drafts (50), Flagged, Sent
- Mailboxes:** Mailboxes, Inbox
- Top Hits:**
 - Serenity Sandford** 2020-08-28
Position: Mental Wellness Support Worker
Inbox - manitoulin.ca
Serenity Sandford ssandford@wikyhealth.ca Aanii, Our team is looking for a Mental Wellness Support Worker to join our team. We are seeking a qual...
 - Serenity Sandford** 2020-08-28
Position: Mental Wellness Support Worker
Drafts - manitoulin.ca
Serenity Sandford ssandford@wikyhealth.ca Aanii, Our team is looking for a Mental Wellness Support Worker to join our team. We are seeking a qual...
- Header:** Serenity Sandford, Position: Mental Wellness Support Worker, To: Alicia McCutcheon, August 28, 2020 at 12:28 PM
- Body:**

Serenity Sandford
ssandford@wikyhealth.ca


Aanii,

Our team is looking for a Mental Wellness Support Worker to join our team. We are seeking a qualified and motivated individual who could be based in one of the 7 First Nations of Mnidoo Mnising, therefore travel may be required or base office fi

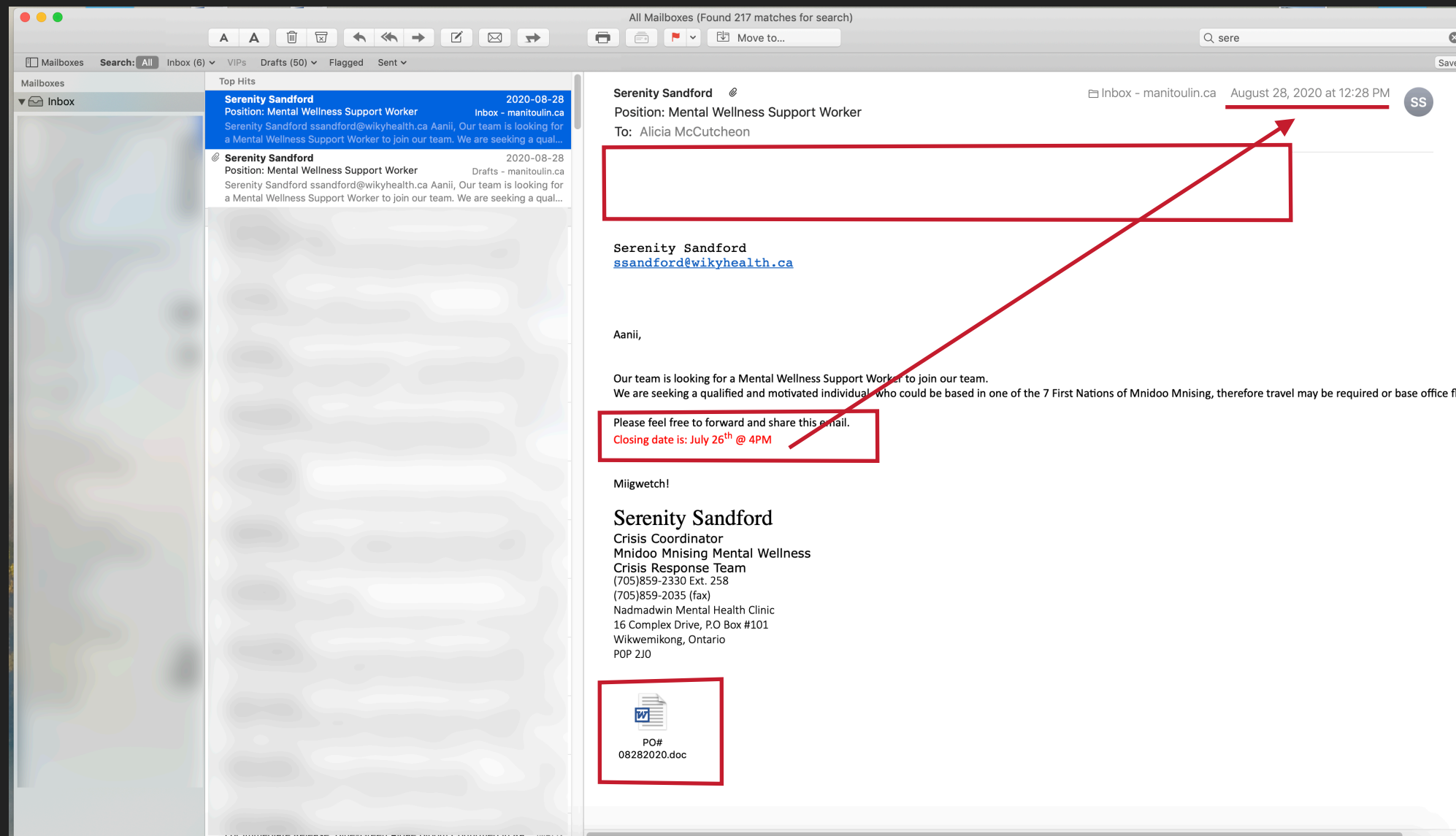
Please feel free to forward and share this email.
Closing date is: July 26th @ 4PM

Miigwetch!

Serenity Sandford
Crisis Coordinator
Mnidoo Mnising Mental Wellness
Crisis Response Team
(705)859-2330 Ext. 258
(705)859-2035 (fax)
Nadmadwin Mental Health Clinic
16 Complex Drive, P.O Box #101
Wikwemikong, Ontario
POP 2J0

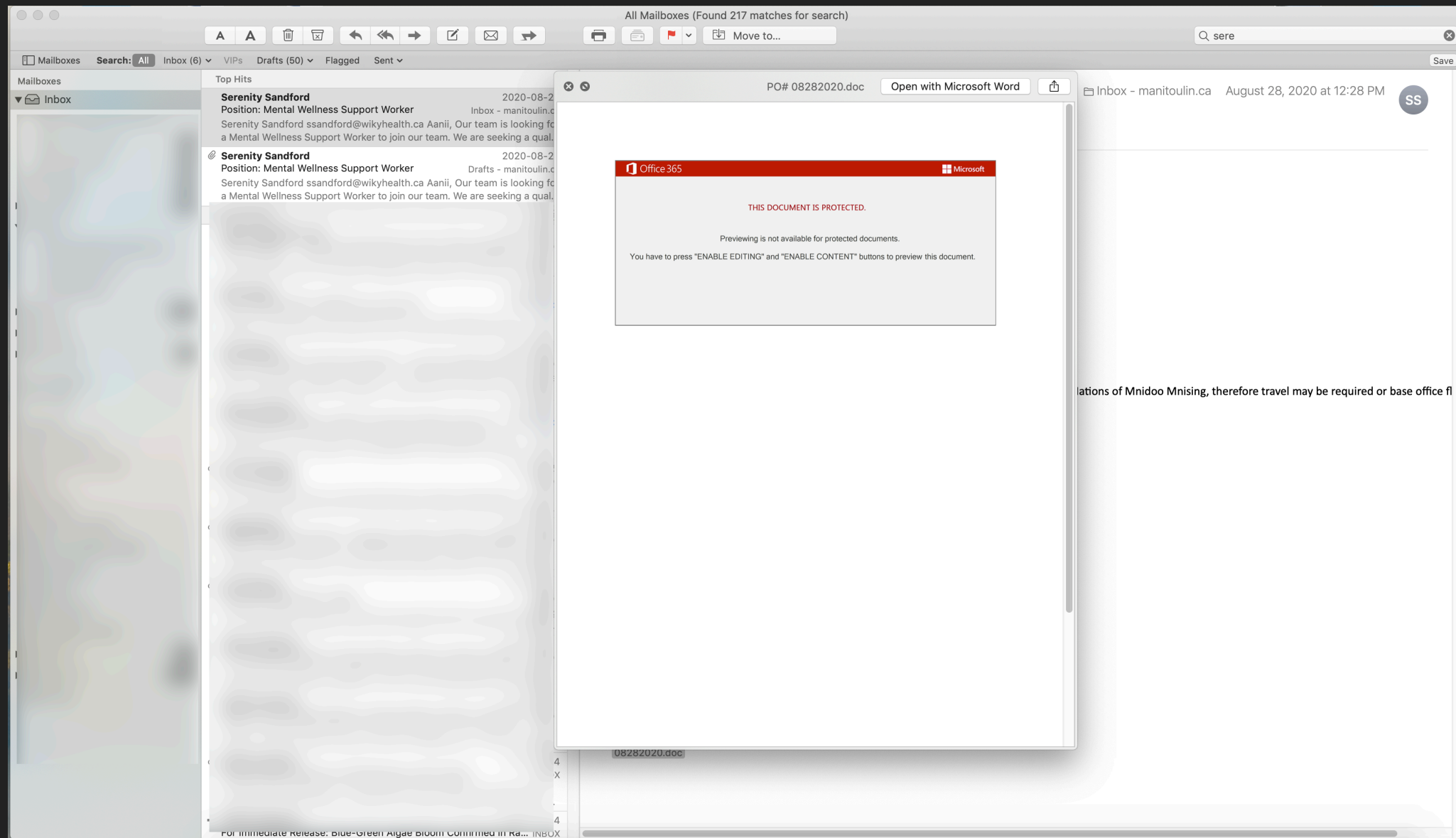

PO#
08282020.doc

EMAIL - SPOTTING THE FAKE



Seemingly a legitimate email from a current client. The first problem that pops out is why is it an apparent forward? Two signatures with the first not matching the second one. Why the blank space at the top? This is a tell-tale sign that the email has been generated and not typed out by hand. Upon closer inspection a number of things just don't add up.

EMAIL - SPOTTING THE FAKE

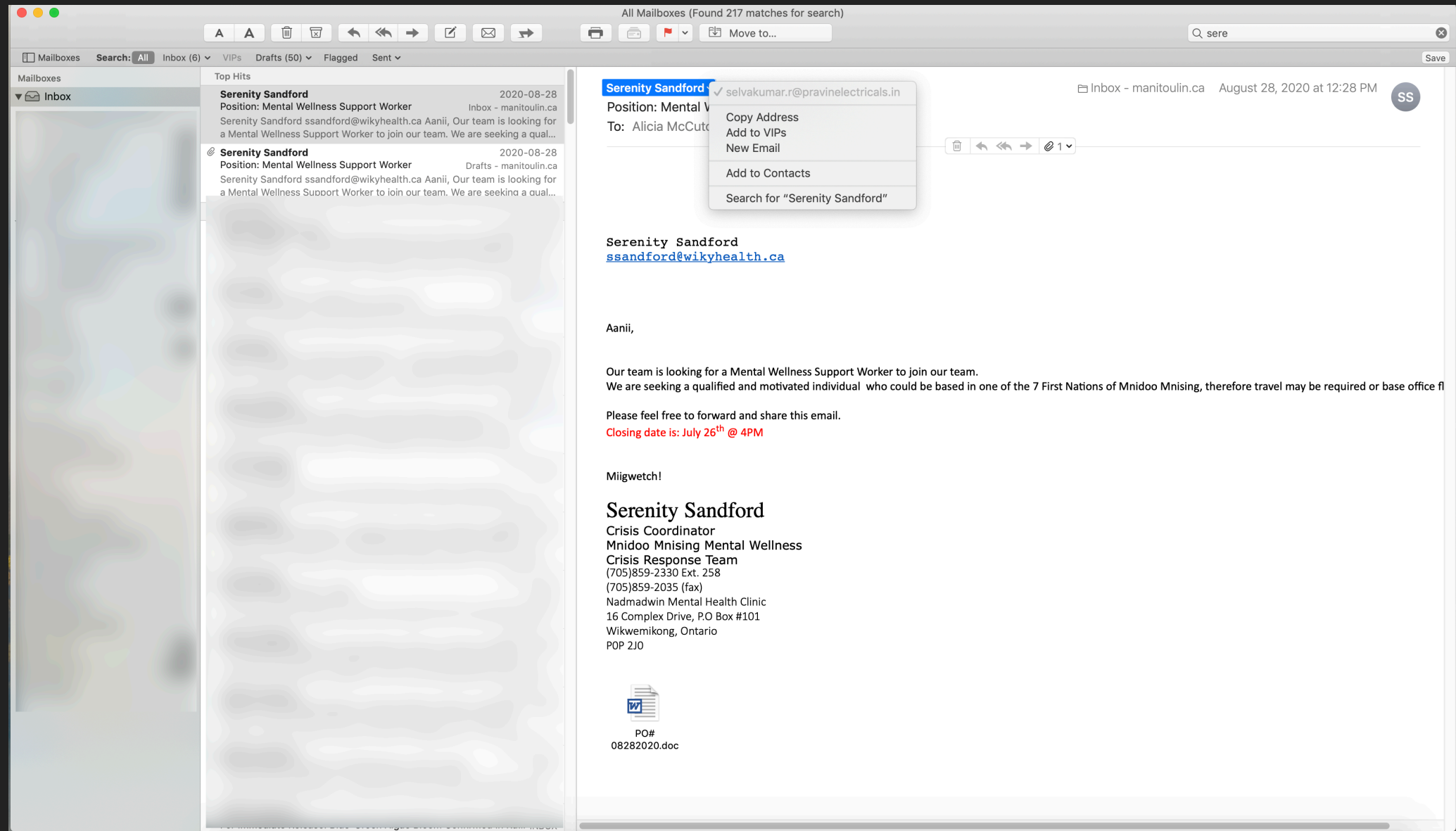


A preview of the attached PO file tells me something is not right. The file is locked and to open it I have to enable editing, 99.99% this is a malicious file.

I run exclusively on an OSX environment so we can preview attachments without executing them.

Do not try this if you are running Windows!

EMAIL - SPOTTING THE FAKE



The final check is the actual source email address. The email originates from selvakumar.r@parvinelectricals.in. Very sure they are not looking for a Mental Wellness Support Worker!

QUESTIONS

This presentation is merely the tip of the iceberg. I encourage questions. No question is stupid, only those that don't ask them.