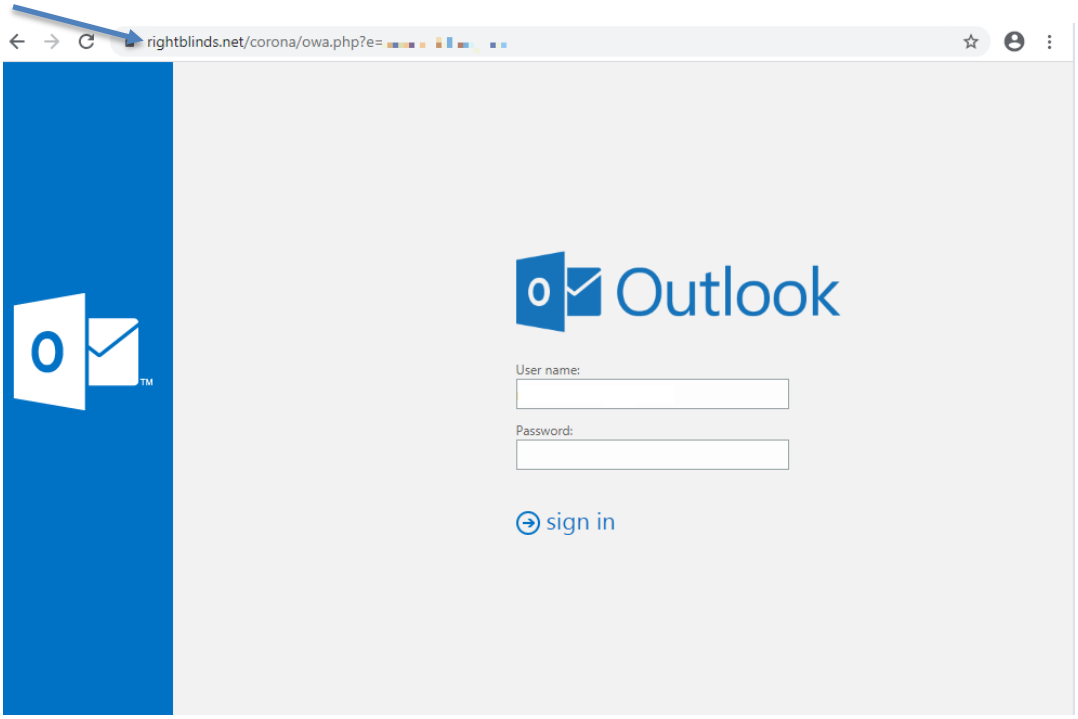
Online caution is needed during the COVID-19 pandemic

Many news outlets are reporting a rise in online and telephone fraud during the COVID-19 pandemic. Catholic Social Services' staff are encouraged to be extra careful when opening email and responding to unfamiliar text messages and phone calls.

Examples of online and phone phishing scams currently circulating, include:

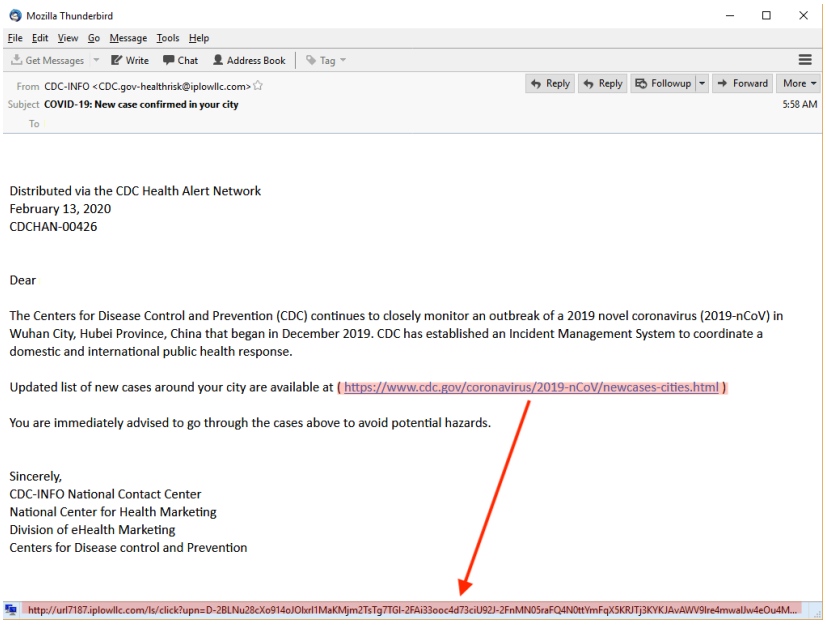
- Be aware of false claims that a virus has spread to the victim's home cities, then prompts users to enter their email passwords in order to read more information.
- Do not click on links. Some fake emails are asking for information, and then uses malicious links to direct victims to a fake Microsoft Outlook portal that steals their login information.



- The Canadian Red Cross has issued a warning against clicking any links in text messages or emails offering masks and claiming to be from their organization as these are fake.
- Scams are circulating from fake charities posing as a government program claiming to be raising funds for the development of a COVID-19 vaccine.
- There have also been recent reports of telephone calls that appear to be from the COVID-19 Information Service at 1-833-784-4397. These calls are fraudulent and were not placed by the Government of Canada. **Never give out personal information if you didn't initiate the call.**
- The Canadian Anti-Fraud Centre says you should be wary of false or misleading information, high-priced or low-quality items, and anything that is presented as a "miracle cure." As well, stay cautious around unsolicited medical advisory emails. The Centre warns of other scams including private companies offering fast COVID-19

tests for a price (only medical professionals can perform the test) or fraudsters urging people to invest in “hot new stocks” related to the illness.

- Be aware of emails with links claiming to be from the World Health Organization or the Centers for Disease Control and Prevention.



Overall, always: Report all suspicious emails to **ReportSuspiciousEmails@cssalberta.ca** and then delete them.

Remember:

- Always check the “from” address in emails before opening them. Do not open emails from senders you do not know and trust.
- Never click on suspicious links or attachments.
- Beware of imposters. Scammers often create email addresses, links and websites that look like well-known companies such as Canada Post and try to trick you. Verify the email address and make sure your dealing with the real thing.
- Don’t believe your Caller ID. There is a software readily available on the Internet to mask or provide a fake caller ID. If the caller seems suspicious, end the call and call back directly from the number in your files or posted on their public website
- Be suspicious of communications that attempt to create a sense of urgency. If an email or caller is trying to pressure you to act or decide immediately, it’s likely not legitimate.
- Never provide your personal or financial information until you have verified the contact information independently.