This bulletin was prepared to warn the public about a new variation of a Tech Support Fraud.

The Canadian Anti-Fraud Centre has received reports of fraudsters sending emails to victims with fake invoices in an attachment. The invoice will use the names and logos of antivirus, tech support and internet payment service companies. The invoice will claim that your subscription has automatically renewed or that there has been an issue with your payment. Fraudsters will provide a phone number for victims to call in order to cancel the service or resolve the "issue". If the victim calls the phone number, suspects will ask for remote access to the victim's device and may ask you to log in to your online banking. By doing this, they will be able to steal your personal and financial information.

Warning signs and how to protect yourself

- Never open attachments from unsolicited emails as these can contain malware or viruses.
- Never allow an unknown person to gain remote access to your computer/device.
- Always look for the legitimate contact information for your service providers.
- Be suspicious about unsolicited phone calls, pop-ups and emails stating your computer/device is infected with a virus or that a threat has been detected.
- Tech support fraudsters will often use "search engine optimization"; they will often be in the first results of your online search.
- Always confirm your service provider's domain and contact information before making a phone call or sending an email.
- Never log in to your bank accounts or email when using remote access applications or sharing your screen with someone.
- Learn [more tips and tricks for protecting yourself](#)

Anyone who suspects they have been the victim of fraud or cybercrime should report it to their local police and to the CAFC's [online reporting system](#) or by phone at 1-888-495-8501. Even if you are not a victim, report it to the CAFC anyway.