HELP DESK QUICK CONTACT

TELECO
Integrating Technologies

MEET YOUR SUPPORT TEAM!

Sean Andrew-Cotter

Chris Cannon

Chris O'Gorman

Shane Smith

Geoff Holtby

1

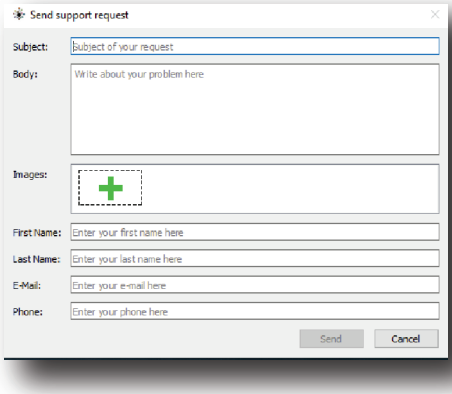
Locate your "Teleco Support Tool" in your task bar.

2

Left click the tool and select "Help Request Form".

3

Fill out the form, screenshots are helpful!



HELP DESK ALTERNATIVE CONTACT METHODS

807-346-7295

Monday – Friday, 8:00am – 4:30PM EST

BUSINESS CRITICAL:

A complete loss of service or a significant feature that is completely unavailable, and no workaround exists.

helpdesk@teleco.ca

Monday – Friday, 8:00am – 4:30PM EST

DEGRADED SERVICE & GENERAL ISSUES:

Intermittent issues and reduced quality of service. A workaround may be available.

TELECO
Integrating Technologies

HELP DESK - DARK WEB COMPROMISE

Dark web monitoring is a process of searching for and monitoring information found on the dark web. It finds stolen or leaked information, such as compromised passwords, credentials, intellectual property and other sensitive data. If a compromise is found for your company through our monitoring you will receive the following email from our Teleco Help Desk.

Subject: Dark Web Compromise

Your email address was found in one or more compromised records.

Details for [email address]:

Site: [origin1]

Password: [password1]

Site: [passwordx]

Password: [originx]

To keep your data safe we highly recommend changing your password for any sites or software that use ANY of the above passwords. Also change your password for any sites listed above or sites that use the same password even if a password is not listed.

We highly recommend using long (>15 characters) unique passwords for each site or software and a password manager such as Bitwarden to store and create the passwords. For getting started guides for Bitwarden click here or go to https://bitwarden.com/help/getting-started-videos/ in a browser. As well use Multifactor authentication (MFA) if provided by the site or software.

Please contact us at helpdesk@teleco.ca for assistance in setting up Bitwarden or guidance on password management and MFA.

NOTE: Please Reply All if you wish to discuss information or have questions relating to this email.

TELECO
Integrating Technologies

HELP DESK – SUSPECTED PHISHING EMAIL

We provide advanced protection on email security and protect your inbox using API, machine learning and Artificial Intelligence (AI). All emails, files and attachments are scanned before hitting your inbox and the AI is continuously learning to improve security. If a phishing email is suspected it will be quarantined and you will receive the following email from our Teleco Help Desk.

Subject: Quarantined

Hello “User”

An email has just been received from Dylan Banks <echirino@sudebip.gob.ve> and is suspected to be a "Phishing" email.

The email message is safely quarantined.

The email subject is: Fw:

Email attached files are:

Detection reasons are:

If you wish to request to release it from quarantine, click here.

You can read more about phishing attacks here.

HELP DESK - ABNORMAL EVENT

Teleco monitors your IT network to ensure that it's operating efficiently and securely. In doing so we react to routine and unexpected events that require our attention. If something is flagged as abnormal or unusual, we will contact you for further clarification. For example, we may suddenly see your user profile log in from Italy which is unusual until we find out you are vacationing there. If abnormal or unusual activity is detected, you will receive the following email from our Teleco Help Desk.

Subject: Abnormal Event

We have detected abnormal activity with your account that seems out of the ordinary. If you are travelling or have any explanation please let us know by responding back to us by reply back to this email or contacting us at helpdesk@teleco.ca.

Do you use a VPN that may account for this event? If you are unaware of any possibility that this event is valid then we recommend that you change your password and use MFA (multi-factor authentication). If you use the same password for any other website or software please change those resources.
We highly recommend using long (>15 characters) unique passwords for each site or software and a Password Manager such as Bitwarden to store and create the passwords. For getting started guides for Bitwarden click here or go to https://bitwarden.com/help/getting-started-videos/ in a browser.

Please contact us at helpdesk@teleco.ca for assistance in setting up Bitwarden, guidance on password management or MFA.

NOTE: Please Reply All if you wish to discuss information or have questions regarding this email.