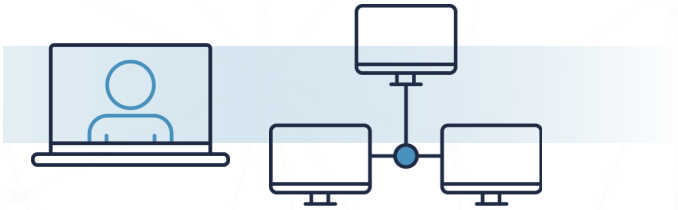
VIDEO-TELECONFERENCING

MAY 2020 ITSAP.10.216

By using video-teleconferencing (VTC) applications, your organization can meet and work with employees, clients, and partners who are in different geographic locations. However, there are security and privacy risks that you should consider before selecting and implementing VTC applications in your organization. Identifying the threats and risks related to these tools ensures that you implement the appropriate security measures and best practices to protect your organization's virtual work environment.



BENEFITS

VTC applications can increase productivity and improve collaboration between your employees, clients, and partners. These applications are more engaging than phone calls and offer face-to-face interaction between participants. Many of them have built-in collaboration tools (e.g. screen and file sharing, recording capabilities).

You can host meetings of various sizes without needing the physical space to do so.

There are many applications that are available for free or offer subscription options with a sliding fee scale, depending on the services that your organization needs.

RISKS

There are a lot of VTC applications to choose from. The security of your organization's systems and information is affected by how the vendor prioritizes security and how you use and secure these applications.

Threat actors can take advantage of vulnerabilities and software flaws and use brute force attacks to steal information or gain access to private discussions.

If sensitive information is discussed or shared on a VTC application, you may be at a higher risk of a data breach or a privacy breach, which can jeopardize your organization's reputation and relationships with clients and partners.

THREATS

Threat actors are targeting VTC applications to disrupt meetings, overload services, eavesdrop on calls, and steal information. Threat actors use different methods to attack VTC applications:

- **Brute-force attacks:** A threat actor automatically scans a list of possible meeting IDs to try to connect successfully.
- **Meeting bombing:** A threat actor joins a meeting to listen in on the conversation or disrupt the meeting by sharing inappropriate or explicit content.
- **Screen scraping:** A threat actor collects screen display data from a compromised system.
- **Malware**: A threat actor can infect devices by sharing malicious attachments, links, or applications to malicious hosts (e.g. websites, software).
- **Phishing**: A threat actor may attempt to initiate a VTC by imitating a trusted contact (e.g. with a non-functioning camera).
- **Insider threat:** Vendor personnel may accidentally or purposely compromise your organization's VTC meetings. An employee may mistakenly share information (e.g. meeting credentials) without having the proper training.

Never share sensitive information over VTC applications. Use other methods if you need to share sensitive information (e.g. secure encrypted messaging).

AWARENESS SERIES

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

SECURITY BEST PRACTICES

To mitigate the risks associated with using VTC applications, your organization needs to take precautions when selecting, implementing, and using the application. Consider the following tips:

CHOOSE THE APPLICATION

- Download applications from trustworthy vendors.
- Use existing corporate solutions whenever possible.
- Use a VTC application with security controls that can be customized to meet your requirements (e.g. security controls may differ between free and paid versions of the application).
- Use vendors that abide by Canadian privacy laws to ensure your information is protected from unauthorized users and sharing.
- Test the application before organizational use.

SECURE THE APPLICATION

- Keep applications up to date or consider using a solution that does not require participants to install software unless necessary (e.g. VTC web versions do not require user updates).
- Change default settings, as they are often less secure.
- Disable features you are not using (e.g. file sharing, screen sharing, transcript generator).
- Ensure administrative privileges are restricted to those who require them.

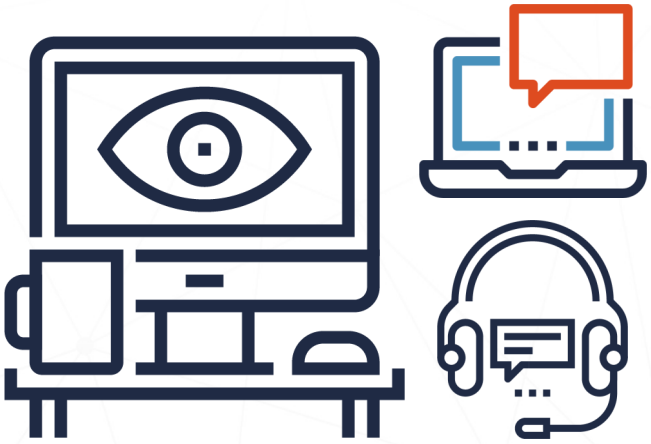
SECURE YOUR MEETINGS

- Secure a meeting with a passphrase or password.
- Keep the meeting link and password private.
- Ensure participants can only join the meeting if the host is present.
- Use a waiting room for participants, if available.
- Keep the number of meeting administrators or hosts to a minimum.
- Never share or discuss sensitive information on teleconferencing applications.

INCIDENT RESPONSE

If you suspect any malicious activity on your VTC meetings:

1. Stop the meeting.
2. Identify the information at risk (i.e. sensitive business or personal information shared in the meeting).
3. Change meeting IDs and passwords for any recurring or scheduled meetings.
4. Report activity to Cyber Centre: **contact@cyber.gc.ca**



TIPS FOR YOUR EMPLOYEES

Security training is an effective way to protect your organization from cyber threats and create a strong security culture. You should remind employees of the following best practices before they use VTC applications:

- Use only approved VTC applications for work purposes.
- Never share sensitive information over VTC.
- Keep the meeting ID and password private.
- Use strong passphrases for accounts.
- Use multi-factor authentication if available.
- Type the VTC web address manually into a web browser to avoid clicking on potentially malicious links.
- Use a secure Wi-Fi network.

See our related alert, *AL20-011 Considerations when using video-teleconferencing products and services,* which is available on our website.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**