

COMPUTER SECURITY CONSIDERATIONS DURING COVID-19

alexioTM

Alexio Corporation is a global award-winning healthcare cybersecurity company, and we're here to help

[BOOK A FREE CONSULTATION](#)

getalexio.com

Alexio is a registered trademark of Alexio Corporation

COVID-19 SCAMS

Be on the lookout for:

- Fake coronavirus tracking maps
- Fake emails with coronavirus updates, links
- Text messages with links to find people in your area with coronavirus
- Ads for coronavirus home-testing
- Websites to register for coronavirus updates
- Facebook posts with fake cures and links to find out more
- Phone scams

Below are legitimate links for COVID-19:

<https://www.who.int/emergencies/diseases/novel-coronavirus-2019>

[https://www.canada.ca/en/public-health/services/diseases/coronavirus-](https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html)

[disease-covid-19.html](https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html) [https://www.ontario.ca/page/2019-novel-](https://www.ontario.ca/page/2019-novel-coronavirus-ontario-only)

[coronavirus - Ontario ONLY.](https://www.ontario.ca/page/2019-novel-coronavirus-ontario-only)

<https://www.cdc.gov/coronavirus/2019-ncov/about/index.html>

[https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insigh](https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf)

[ts_risk_management_for_novel_coronavirus.pdf](https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf)

REMOTE WORKING TIPS

- Use a computer with a current operating system
- Keep security updates done (look up how to do this as automatic updates can't be relied on) NOTE: If you are an Alexio subscriber this is already done for you.
- Ensure you're using proper antivirus software and that it is continuously updated NOTE: If you are an Alexio subscriber this is already done for you.
- Have a business grade firewall. Do not share with others that have unprotected devices, or use DNS filtering to protect your connection.
- Get security awareness training especially for phishing and ransomware.
- Do not share your computer.
- Use only a secure encrypted remote connection like Logmein, Alexio Connect, or a monitored VPN for remote connection NO RDP
- Use unique passwords for each online account. Password managers are very helpful.

Article: Healthcare IT News Telehealth, Remote Work Privacy & Security

<https://healthitsecurity.com/news/must-have-telehealth-remote-work-privacy-and-security-for-covid-19>

TELECONFERENCING TIPS

For Healthcare workers, check with your regulatory college for guidelines. Below are general recommendations:

- Choose a service with E2E (end to end) encryption
- Password protect your meeting links
- Do not record without consent
- Do not record to an unencrypted computer
- Keep systems up to date & encrypt if you're going to save any patient data to it. [How to encrypt DIY](#)

NIST Standards: Securing Remote Telehealth PDF

<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>