Remember, you're not in the office!!

TELECOMMUTING

Are you secure??

For example

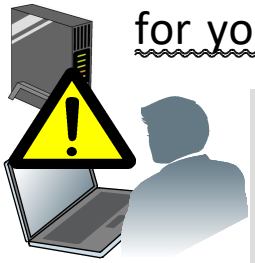
Your device could be infected with a computer virus through a website or application, and your information stolen.

*Please keep your device and anti virus software updated!

Wi-Fi hotspots in public spaces such as cafes do not have sufficient security, and your communication might be intercepted.

Communication using Wi-Fi hotspots (public wireless LAN) increases the risk of interception. Please be sure to turn the file-sharing service off, and unless the connection is encrypted (VPN), refrain from sending any information that could be harmful if leaked or stolen.

If you haven't changed the original pre-set ID and password for your home Wi-Fi router, your PC may be hacked.



If you are not sure whether the initial ID and password have been changed, check the router settings. If they are still set to names such as "Admin" or "Password" then your connection may not be secure. Be sure to change them to something not easily guessed.

OTHER TIPS

- Don't reuse your passwords.
- Be careful about peep into your device and theft in public place.
- Confirm with your office about teleworking protocol in advance.

Hokkaido Prefectural Police

Cyber Security Control Task Force

サイバーセキュリティひろば Search

Hokkaido Prefectural Police

*Portions of this flyer have been edited for clarity.