Working from Home Script

The world of work is rapidly changing, and many of us are working from home more than ever before.

When you work in the office, you benefit from security measures that protect our networks, systems, devices, and information from cyber threats.

Moving from a trusted office environment to remote work locations can create security risks.

In this video, you will learn how you can help keep Ontario's information secure while working from home.

The first source of risk we are going to examine is your devices.

It is important that you only work from issued devices assigned to you by your manager. Issued devices are for business only - avoid all personal use unless you have manager approval.

Work information should not leave your work devices, so DO NOT forward work information to your personal devices, unless formally approved by your manager, and DO NOT share your work assets with anyone.

If work assets are lost or stolen, report the loss immediately to your manager and your organization's IT service desk or support chat.

The second source of risk we will examine is your home network.

Your home Wi-Fi network is critical to making your workspace cyber secure.

One of the easiest ways to increase your home cyber security is to change your Wi-Fi password from the default that comes with your router and to use a strong password that is difficult to guess.

The final source of risk we are going to examine are phishing emails.

Phishing email messages often try to create an impression of urgency in order to scare you into clicking on a link or divulging information.

You should always be suspicious of any email asking you to update your passwords and login credentials.

If you suspect an email is a scam, research and contact the organization directly to see if it was sent by them.

Thank you for watching!