Cybersecurity awareness

July 2025

Key Messages

- The Government of Saskatchewan is committed to increasing cybersecurity awareness across government and is implementing mandatory cybersecurity awareness courses for all employees.
- The mandatory courses will ensure employees are aware of current risks and have the necessary knowledge to mitigate them.
- The mandatory courses will be reviewed, updated and delivered annually.
- In 2025-26, employees with a gov.sk.ca email account are required to complete the following courses:
    - Social Engineering training;
    - Remote Working training;
    - Artificial Intelligence training;
    - User Acceptable Usage Policy acknowledgement; and
    - Overarching Security Policy acknowledgement.
- Starting July 24, employees will receive emails from csrm@gov.sk.ca with a link to launch the courses.
- The courses are delivered on the MetaCompliance platform and do not require employees to provide any login information.
- Each course will take approximately 10 minutes to complete.
- For more information, visit Taskroom.

Questions and Answers

Why do I need to complete the mandatory cybersecurity awareness courses?
The courses will help improve cybersecurity awareness among users of Government of Saskatchewan (GOS) information technologies and applications. Completion of these courses will ensure employees are aware of current risks and have the necessary knowledge to mitigate them. The courses are mandatory and must be completed by all employees by March 31, 2026.

What is included in the cybersecurity awareness courses?
Courses may include important information, videos and quizzes. Some may require you to acknowledge you have read a policy by selecting a button.

When will I receive the cybersecurity awareness courses?
Starting July 24, 2025, employees will start receiving emails from csrm@gov.sk.ca. Reminders will be sent quarterly to users who have not completed the courses.

How long does it take to complete the cybersecurity awareness courses?
Each course can be typically completed in 10 minutes.

Cybersecurity awareness

July 2025

How do I complete the cybersecurity awareness courses?
You will receive emails from csrm@gov.sk.ca. When you click the "Launch Course" link in the emails, it will direct you to the MetaCompliance platform. The course will begin when you click the play button on the video. Please follow all instructions on the screen to complete the courses.

How will I know if I have completed a cybersecurity awareness course?
Upon completion of each course, a thank you message will be displayed, and the user can click on the "Exit Course" button. Users will be redirected to their course dashboard. Users can then click on "Training" or "Policies" to see a list of completed and incomplete training and policy courses. Users can return to their dashboard by clicking on the home button on the left-hand bar in the MetaCompliance platform.

When do I need to complete each of the cybersecurity awareness courses?
The deadline for completion is March 31, 2026; however, users are encouraged to complete the courses at their earliest convenience. Users will stop getting quarterly reminders once they have completed the courses.

What happens if I do not complete a cybersecurity awareness course?
Course completion is mandatory. Users will receive quarterly reminders for incomplete courses.

Will it show in PSC Client that I have completed the courses?
Information is not shared between MetaCompliance and PSC Client and courses will not be shown in PSC Client.

How can I check if I have completed all the necessary courses?
Access the MetaCompliance platform using the course emails. Click on the home button on the left-hand bar to take you to the dashboard. Users can then click on "Training" or "Policies" to see a list of completed and incomplete training and policies courses. In addition to the five new mandatory courses, there may be other courses that have been sent to you in the past.

What happens if I do not pass the quiz?
Employees are not required to pass the quiz. The interactive quiz is to validate knowledge of the associated course. The results of the tests are revealed to the user immediately after a section is completed, regardless of the outcome (pass/fail). Completion of the course is not impacted by the results of the quiz.

What do I do if I accidentally delete the email with the link to a course?
There are a few options to find the link to your courses if you delete the emails:

- Check your trash folder in Outlook. Emails are often sent to the trash folder before being permanently deleted. You may be able to find it there.
- Click the link in an email for one of the other courses. Once you are in the MetaCompliance platform, click the home button on the left-hand side, which will take you to your dashboard. Users can then click on "Training" or "Policies" to see a list of completed and incomplete training and policies courses. Click on an incomplete course to begin.

- Email the SaskBuilds and Procurement Cybersecurity and Risk Management branch at SBPITInformationSecurityBranch@gov.sk.ca requesting for the course to be sent again.
- Lastly, employees can wait for the quarterly reminder emails and take the course then.

Will I need to take the course every time I change positions within government and a new login account is created for me?
No. Although the user would get an email stating they have not completed the cybersecurity awareness courses, the Cybersecurity and Risk Management team can mark it as completed if you notify them at sbpitinformationsecuritybranch@gov.sk.ca.

Will the cybersecurity awareness courses change each year, or will the topics remain the same?
The mandatory courses will be reviewed, updated and delivered annually.

What other policies should I be aware of that aren't covered in these courses?
All GoS information security policies are provided on Taskroom's Information Security Policies page.

What other cybersecurity topics should I be aware of that aren't covered in these courses?
Users could explore a variety of topics including, but not limited to:

1. Ransomware Attacks: These are when hackers lock your files and demand money to unlock them. Sometimes, they also threaten to release your private information if you don't pay.
2. Nation-State Attacks: These are cyberattacks by countries targeting other countries' government agencies and important industries to steal information or cause disruptions.
3. Internet of Things (IoT) Device Risks: Many everyday devices like smart thermostats and security cameras are connected to the internet. Hackers can exploit weaknesses in these devices to gain access to your network.
4. Artificial Intelligence (AI)-Powered Attacks: Hackers are using AI to make their attacks smarter and harder to detect.
5. Geopolitical Cyber Threats: Political tensions between countries can lead to cyberattacks, including spreading false information online.
6. Supply Chain Attacks: Hackers target third-party vendors that companies rely on, which can cause widespread issues if those vendors are compromised.

A good source for information on these and other topics is Get Cyber Safe.

Who can I reach out to for questions?
Any questions can be directed to your manager or SaskBuilds and Procurement's Cybersecurity and Risk Management Branch at: SBPITInformationSecurityBranch@gov.sk.ca.