

Key Messages and Questions and Answers – MetaCompliance

KEY MESSAGES

- The Government of Saskatchewan’s Information and Technology Division is introducing two new initiatives to help strengthen cyber security across government:
 - A new “Phish Mail” button will automatically appear in your Outlook toolbar on December 16, 2022. To report phishing or other unsafe emails to the IT Service Desk, click the “Phish Mail” button, then click “Report”.
 - New cyber security education courses will be sent to all Government of Saskatchewan employees by email on a regular basis, beginning in January 2023.
- Completion of the cyber security courses is mandatory for all government employees. Reminders will continue to be sent to employees until courses are completed.
- These emails will come from the Cyber Security and Risk Management team email (csrm@gov.sk.ca) and will include a “log in” button that links to a platform called MetaCompliance. There is no need to enter login details to take the training.
- For any questions, please reach out to the Cyber Security and Risk Management Branch at csinformationsecuritybranch@gov.sk.ca.

QUESTION AND ANSWERS:

Q: Why is there a new Phish Mail button added to my outlook email toolbar?

A: A new button will be added to the outlook toolbar for reporting dangerous or phishing emails to the government’s cyber security team. This is being done to help ensure potentially dangerous emails are reported to the Cyber Security and Risk Management Branch quickly and routinely, so they can take next steps to address them before they become a problem.

Q: What devices will the new Phish Mail button be added to?

A: The new button will be added to all Government of Saskatchewan (GOS) Outlook user’s accounts. Any device that accesses a GOS Outlook email account will have the new button automatically added to the Outlook toolbar.

Q: What happens to an email that is reported as suspicious or phishing. Is it deleted from my inbox?

A: When an email is reported using the Phish Mail button, it is removed from the user’s inbox and forwarded to the Cyber Security and Risk Management Branch at csinformationsecuritybranch@gov.sk.ca for further investigation.

Q: I am unsure if an email is safe to open or not. Do I press the new Phish Mail button to report it?

A: Yes. If you cannot confirm who sent the email, or the contents of the email, it is best to err on the side of caution and report it for further review by the cyber security team.

Q: Do I have to report messages using the new Phish Mail button?

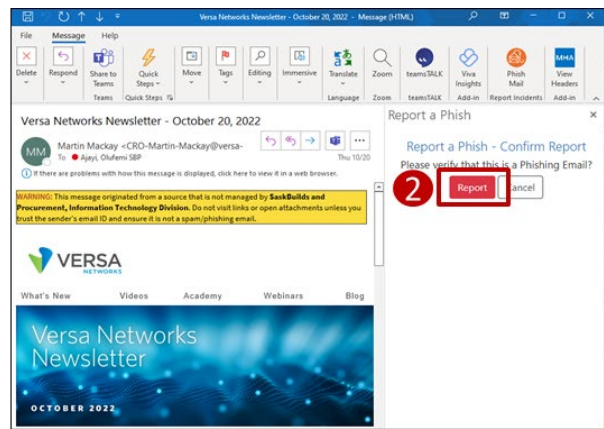
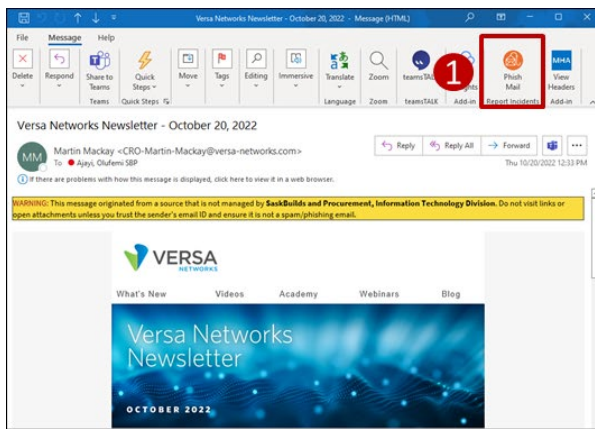
A: It is the responsibility of all government employees to ensure that they do their best to maintain cyber security. We recommend employees take advantage of the new safety tool and report any suspicious or dangerous emails.

Q: When will the new Phish Mail button be added to my Outlook toolbar for reporting suspicious emails?

A: The new Phish Mail button will be added to all outlook toolbars on December 16, 2022.

Q: How do I use the new Phish Mail button?

A: If you think an email is suspicious or a phishing attempt, simply press the new button at the top of your Outlook toolbar labeled “Phish Mail”, then click “Report”. This will automatically report the email to the government’s cyber security team for their review.



Q: How do I complete the new MetaCompliance courses?

A: MetaCompliance courses can be completed online using the link sent by government’s Cyber Security and Risk Management Branch to your email. To complete a course, simply press the “Login” button at the bottom of the email body.

Q: How will I know I have completed a MetaCompliance course?

A: An instant notification will be sent to users upon course completion.

Q: What happens if I don’t complete a MetaCompliance course?

A: If you haven’t completed a MetaCompliance course, you will continue to receive email reminders until the course is completed.

Q: Can I opt out of enrolling in MetaCompliance courses?

A: No. All government employees will be automatically enrolled in the new courses in an effort to further strengthen cyber security across government.

Q: How long does it take to complete MetaCompliance courses?

A: Courses typically take users 10 to 20 minutes to complete.

Q: What is included in a MetaCompliance course?

A: Courses are typically made up of five parts: an introduction video, an educational video, interactive content to test your learning, an encouragement image, and a closing video.

Q: What happens if I do not pass the interactive test?

A: Interactive content is education, not Pass/Fail. Users are encouraged to do their best, but test scores are not recorded and all users pass interactive tests by simply participating.

Q: When will I receive enrollment for my first MetaCompliance course?

A: The first MetaCompliance course will be distributed on January 11, 2023.

Q: Who can I reach out to for questions?

A: For any questions, please reach out to the Cyber Security and Risk Management Branch at csitinformationsecuritybranch@gov.sk.ca.