

Questions and Answers: August 2026 cybersecurity incident

This document provides additional information about the Aug. 18 cybersecurity incident and guidance for employees. It will be updated as more information becomes available.

About the incident

What happened?

On Aug. 18, 2026, SCS experienced unauthorized access to and encryption of its computer systems. SCS immediately took steps to isolate the threat, restore access to systems, and engage independent cybersecurity specialists to investigate.

What did the investigation find?

The investigation confirmed an unauthorized third party gained access to and encrypted SCS's systems.

The investigation could not determine whether client personal information was accessed. While there is no evidence that client information was viewed, copied, or misused, we cannot completely rule out potential access to individual files and associated client information.

Has any personal information been misused?

We have no evidence client information has been misused. However, the investigation could not rule out potential access to client information.

What is SCS doing to prevent another incident?

We have assembled a dedicated incident response team consisting of internal and external experts. We are reviewing our systems and implementing additional security measures to reduce the risk of a similar incident.

Impact on clients and families

Why are we notifying clients and families?

We are notifying clients and families as a precaution and in the interest of transparency.

Although the investigation could not confirm that client information was accessed, it also could not rule out that possibility. We want everyone to be aware of the incident and take appropriate precautions.

Was specific personal information stolen?

The investigation did not find evidence that client information was viewed, copied or misused. However, it wasn't possible to rule out that some personal information may have been accessed. That's why SCS is notifying clients and families as a precaution.

What precautions can I take to protect my personal information?

While we have no evidence that personal information has been misused, we encourage you to:

- **Watch for suspicious communications:** Be cautious of unexpected requests for personal or financial information.
- **Protect your passwords:** Use strong, unique passwords and enable multi-factor authentication where available.
- **Monitor financial accounts:** Check for unusual transactions and report them to your financial institution.
- **Avoid suspicious links:** Don't click on unfamiliar links or attachments.
- **Report concerns.** Contact ITsecurity@scsonline.ca if you notice suspicious activity from SCS.

Additional information

Has the incident been reported to the appropriate authorities?

SCS has advised the Information and Privacy Commissioner of Ontario of the incident.

Where can I get more information?

For questions about the incident, please contact ITsecurity@scsonline.ca.