Internal Q&A

What happened?
We recently became aware that some operational company and employee information was accessed in a recent cybersecurity incident targeted at Bell Technical Solutions. Bell Technical Solutions took immediate steps to secure affected systems.

What company data was compromised/lost?
Some operational company and employee information was accessed in a recent cybersecurity incident targeted at Bell Technical Solutions, including employee emails. Bell Technical Solutions took immediate steps to secure affected systems.

Based on our investigation, we now know that the incident may have affected certain of your personal information. The affected records may have contained certain information, such as:

- Name
- Address
- Telephone number
- Date of birth
- Government-issued ID (such as social insurance and driver's licence numbers)
- Medical information (such as WSIB forms and medical evaluations)
- Banking information (such as sample cheque for pre-authorized debit)
- Other information contained in your employee file (such as performance reviews or information on compensation)

I use my corporate email for personal use. Should I be worried?
If you used your corporate email for private matters such as tax filing, sharing bank information or other such transactions, your private information may have been accessed.

What steps should I take and will you provide additional support if you suspect my private information has been accessed?

Our HR team is here to support you and has set up a contact line for any additional questions you may have. In addition, we will be following up with any employees whose private information may have been accessed. All employees and former employees will be offered credit monitoring services.

Credit monitoring services will be provided to the following individuals:

- All active employees
- Any retiree or former employees
- Any employee on leave or benefits

Can my family members obtain a security token from Equifax as well?
As the information that may have been exposed pertains to employee records, your family's information should not have been exposed. If you believe a family member's information has been exposed, please contact our Human Resources team who will assess the situation case by case.

What is the Company doing so this doesn't happen again?
While no company is immune from cyber threats, we have robust systems in place to help mitigate attacks from being successful. We immediately took steps to secure affected systems. Looking ahead, we will be taking additional measures to enhance our security system to prevent attacks. We have recently rolled out a new interactive security awareness training program that will help team members identify security threats and keep our data and networks secure. Our Be Cyber Savvy interactive training includes an Awareness, Perceptions and Behaviours assessment, learning modules and phishing simulations.

Was customer data compromised/lost?
The name, address and phone number of customers who booked a technician visit may have been accessed. We will directly notify any individuals whose private information may have been accessed.

No customer information such as credit and debit card numbers, banking or other financial data was accessed in the incident.

How did the Company determine which employees were most at risk and how many employees are on that list?
As this is an ongoing investigation, we can't disclose any additional details about the incident. All employees whose personal information may have been exposed are being contacted by the Human Resources team.

How is the Company contacting former employees?
A letter is being sent to all former employees with the details of the information that may have been exposed, the information on how to obtain a security token with Equifax as well as the HR Support telephone number for additional support.

What is the timeline? How far back does the breach go?
As this is an ongoing investigation, we can't disclose any additional details about the incident. All employees whose personal information may have been exposed are being contacted by the Human Resources team.

What steps do I take and/or who do I contact if I am impacted?

1. Report the incident to your local police and get a file number for future reference.
2. Place flags on all of your bank accounts and change your passwords.
3. Report the fraud to credit bureaus.
4. Contact the **Canadian Anti-Fraud Centre** at 1-888-495-8501 or through the Fraud Reporting System.
5. Contact the Human Resources team at 1-877-817-9645, option 7.

Are other Bell customers affected?
No. BTS is on a separate IT system from Bell. Additionally, as Bell MTS and Bell Aliant have separate field services operations, their customers are also not impacted.

Was the Office of the Privacy Commissioner or other authorities notified?
Yes, we are pursuing our investigation and have engaged the RCMP's cyber crime unit and also notified the Office of the Privacy Commissioner.

Was this a ransomware attack and has any cyber-criminal group claimed responsibility?
As this is an ongoing investigation, we can't disclose any additional details about the incident.

How can I monitor my credit rating?
All Canadian citizens can monitor their credit rating free of charge by visiting the Financial Consumer Agency of Canada website. We are also offering credit monitoring proactively for anyone whose private information may have been accessed and will follow up directly.

What should I do if I believe I have become a victim of identity fraud?

1. Report the incident to your local police and get a file number for future reference.
2. Place flags on all of your bank accounts and change your passwords.
3. Report the fraud to credit bureaus.
4. Contact the **Canadian Anti-Fraud Centre** at 1-888-495-8501 or through the Fraud Reporting System.
5. Contact the Human Resources team at 1-877-817-9645, option 7.

How do I report a phish by email?

1. **Select** the email
2. Click on the **Submit as Phish** button at top of email.
3. Your email is automatically sent to phish@bell.ca and a copy will be moved to your junk email folder.

How do I submit a phish on mobile?

1. **Do not** click any links, download attachments, or forward the message.
2. **Forward email** to phish@bell.ca
3. **Permanently delete** the phishing message and the forwarded message in your sent items.
4. **Avoid** using the “link preview” feature on mobile, as this can compromise your mobile device.