Website Landing Page Content - Posted Wednesday, April 6

We identified an email phishing incident on January 6, 2022, that impacted six internal email accounts.

Upon discovery, we immediately initiated our standard incident response processes - rapidly shutting down access, introducing strengthened security measures, and bringing on external experts to support an investigation.

The incident was contained, and email systems are secure, with all operations running smoothly. As a precaution, the investigation continues, and we will provide further updates as necessary.

Out of an abundance of caution, we wanted to share that some personal information may have been accessed during the incident. This may include your account information, debit or credit card number, SIN, identification, and other financial information.

We took immediate and comprehensive action, including enabling multi-factor authentication, resetting employees' passwords, and blocking the malicious sender emails and/or domains identified during the incident. We will continue to take all reasonable steps to minimize any risks to you arising from the incident. Further, please be assured that there is no evidence of any public disclosure or misuse of your information due to the incident, at this time.

In addition to the above, Northern Savings has reported the incident to law enforcement, appropriate privacy commissioners, and other organizations who can assist with mitigating any risks from the incident. Northern Savings has also implemented several additional safeguards to minimize risks to your information going forward.

Given the immediate and comprehensive actions already taken we consider the risk to members low. However, as a precautionary measure, Northern Savings is offering impacted members identity theft and credit monitoring solution free of charge for two years. To sign up for this service please send an email to inquiries@northsave.com or call us at 250.628.0256 or toll-free at 877.656.9505. There are additional things we recommend you do to protect yourself and your online information:

- Use strong passwords - alphanumeric in nature (a combination of both upper and lowercase letters as well as numbers and special characters).
- Change your passwords regularly.
- Clear your browsing history regularly and at the conclusion of any online banking or other transactions where you make online purchases.
- Sign up for banking alerts that will notify you when your password has been changed or your banking account has been accessed/used.
- Do not click on links, provide money, or confidential information where you cannot independently verify the authenticity of a request.

Thank you for your trust and support.

If you have any immediate questions or concerns, please contact: inquiries@northsave.com

Website Q&A - Posted Wednesday, April 6

1. **What steps has Northern Savings taken to strengthen its email systems? How can you prevent this from happening again?**

Below are some of the changes that we have implemented to best protect your information by strengthening our information security program:

- Northern Savings has reported the incident to law enforcement, appropriate privacy commissioners, and other organizations who can assist with mitigating any risks from the incident. Northern Savings has also implemented several additional safeguards to minimizerisks to your information going forward.
- We have engaged third-party experts to objectively evaluate and make recommendations for

further process enhancements.
- We continue to monitor the dark web and other online locations. To date, no public disclosure of customer data from the attack has been identified.
- We have implemented strengthened cybercrime detection technology across the organization.
- Our teams, organization-wide, have/will participate in annual security and privacy awareness andtraining programs.

2. What services are you offering to protect my information/data?

If you are or were a member or an employee of Northern Savings, some of your information in our e-mail system may have been accessed as a result of this incident. In particular, this may include your account information, debit or credit card number, SIN, identification, and other financial information.

There is no evidence of any public disclosure or misuse of your information. However, out of an abundance of caution, we are notifying you of the incident and as a precautionary measure, Northern Savings is offering identity theft and credit monitoring solutions free of charge for two years. To sign up for this service please send an email to inquiries@northsave.com or call us at 250.628.0256 or toll-free at 877.656.9505.

3. What happened?

We identified an email phishing incident on January 6, 2022. We initiated standard incident response processes, rapidly shutting down access, introducing strengthened security measures, and bringing on external experts to support an investigation. The incident was contained, and email systems are secure, with all operations running smoothly. As a precaution, monitoring continues, and we will provide further updates as necessary.

4. Is my information safe now?

We took immediate and comprehensive steps, and we will continue to take all reasonable steps to minimize any risks to you arising from the incident. Further, please be assured that there is no evidence of any public disclosure or misuse of your information due to the incident at this time.

5. Is the issue contained? Are you sure that any other systems haven't been compromised?

Yes, the issue has been contained. With the help of best-in-class cyber security experts, we are implementing further safeguards to protect your information and reduce the risk of future incidents. Please be assured that there is no evidence of any public disclosure or misuse of your information due to the incident at this time.

6. Should I change my password to my online banking account and app?

Our investigations indicate that our online banking portals and internal systems were not impacted by this incident. However, as best practice, there are additional things we recommend you do to protect yourself and your online information:

- Use strong passwords - alphanumeric in nature (a combination of both upper and lowercase letters as well as numbers and special characters).
- Change your passwords regularly.
- Clear your browsing history regularly and at the conclusion of any online banking or other transactions where you make online purchases.
- Sign up for banking alerts that will notify you when your password has been changed or your banking account has been accessed/used.
- Do not click on links, provide money, or confidential information where you cannot independently verify the authenticity of a request.

7. How do I get in contact with a privacy commissioner to learn about my rights?

While you are entitled to file a complaint with the privacy commissioner, we have already notified them of this incident. Those who have questions about their rights can learn more by contacting the

privacy commissioner in their respective jurisdiction.