SEDA Email Compromise Follow-Up: Updated Information and Actions Taken

Dear SEDA Members and Network Partners,

I am writing to provide you with a comprehensive update following the recent security incident that resulted in phishing emails being sent from a compromised email account.

Our Sincere Apology

First and foremost, I deeply apologize for any inconvenience, concern, or potential security risks this incident may have caused you or your organization. We understand the importance of maintaining your trust in our digital communications.

Immediate Response and Investigation

Following the incident, these are the actions we immediately took to secure our systems and understand the full scope of the breach:

- A notification email was sent out to our Member/Partner distribution list via our web-based distribution channel
- Our IT firm conducted an immediate containment and assessment of the security incident
- An independent external cybersecurity consultant was retained to perform a comprehensive audit of our Microsoft 365 environment and all hardware systems
- All potentially affected systems were secured, permissions and access protocols were reviewed

Investigation Findings

The thorough security audit has provided us with the following insights into the incident:

- The breach was contained within the email environment
- The compromise was attributed to a failure of the Multi-Factor Authentication (MFA) on the affected account

Your Data Security

We want to reassure you about the protection of your information:

- SEDA does not store client or member personal information in digital formats
- Online financial transactions are securely processed directly by a third-party payment processor

- Multi-Factor Authentication was and remains an existing standard on all organizational accounts and has now been remediated and retested. It is also our policy to utilize MFA on all external web-based access points, when MFA is available as an option
- Our cyber insurance policy holder provides monthly scans and assessments of our websites to augment our own monitoring of these assets

Moving Forward

As a result of this incident, we are upgrading our email and hardware security to a more comprehensive endpoint solution.

This incident is a reminder that phishing and spoofing attempts are becoming more common. Phishing, in particular, can give attackers access to your email account credentials just by getting you to click on a harmful link.

At any time in the future, should you have any doubt or concern about any email originating from the SEDA team – be sure to contact us directly by phone (306-384-5817) or via one of the following secure email addresses:

- General Administration seda@seda.ca
- Verona Thibault CEO ceo@seda.ca
- Carmen Hesje, Programs Administrator programs@seda.ca
- Jackie Wall, Manager Special Programs ecdev@seda.ca
- Logan McManus, Membership Coordinator logan@seda.ca

Please feel free to call me directly if you have any questions or concerns about this incident and our upgraded security measures.

Respectfully,

Verona Thibault
Chief Executive Officer, SEDA