Staff Report

Finance and IT Services

Report To: Community Communications Advisory Committee
Meeting Date: November 18, 2019
Report Number: FAF.19.149
Subject: Town of The Blue Mountains Corporate Website and Network Security Precautions
Prepared by: Cathy Bailey, Manager of Information Technology

A. Recommendations

THAT the Community Communications Advisory Committee receive Staff Report FAF.19.149, entitled "Town of The Blue Mountains Corporate Website and Network Security Precautions" for information purposes.

B. Overview

The Community Communications Advisory Committee has asked that the Manager Information Technology (IT) deliver a report explaining the Town's IT security measures.

C. Background

Security is a high priority for the IT division. System monitoring software tells us that the Town's website, data and network infrastructure is under attack at all times from all corners of the globe. There is a requirement for many layers of complex, automated, "best of brand" tools that ensure the Town's systems run without interruption.

In spite of these tools, staff sometimes receive spam messages containing potential attacks. In these cases, IT is forced to rely on the security intelligence of all our staff, council and committee members to avoid attacks.

Ransom attacks have become very frequent in the municipal IT world recently, including some municipalities in our neighbourhood, taking down networks for weeks and sometimes months while ransom is paid and systems are restored to normal operation. These ransom attacks are often enabled by an innocent, internal person who inadvertently clicks on the wrong link in a spam message. One wrong click takes down an entire network. It used to be that these dangerous spam messages were easy to detect, by their odd language and grammar. Now they are difficult to detect and require a high level of vigilance from all users to ensure our systems are safe.

This map indicates the countries that have been attacking the Town's email systems in the last 30 days.

In a **one week** period in July:

- 44,399 messages were sent from the outside to the Town's email systems
- 36,164 were identified as spam or contained viruses
- Only 7,135 messages were delivered to Town staff

D. Analysis

The following are some of the security measures in place and why:

- Internal IT processes, methodologies and procedures are not posted in the public forum
  - Bad actors could use this information to launch attacks
- Use contact forms on the website instead of posting email addresses
  - Robotic attack programs sift through website pages to collect email addresses and then launch attacks by emailing staff. The only way to prevent this is to remove the email addresses from the website and replace them with contact forms
  - Many website users do not have their computer or mobile device programmed so that email links work. Contact forms make the website universally available to all users
- Use captchas on all contact forms on the website
  - Captchas force website users to click on images or type a character sequence they see on the screen. The captcha is different every time someone uses the contact form. This means that robotic attack programs cannot use the contact form to launch an attack on the Town's website. The attack programs submit contact forms without captchas repeatedly in quick succession in an effort to swamp the website so that it can't respond to any other users, essentially taking it down

- Keep the number of staff member names on the website to a minimum
    - Everyone who has their name on the website is a target to bad actors. They will receive more spam which is targeted directly at them. The bad actors will also send messages pretending to be those staff members; these messages are sometimes very hard to detect. In recent weeks this has been happening more frequently
- Send all contact forms to generic group internal email addresses rather than to individuals
    - This is a business continuity effort. Sometimes staff are away unexpectedly; all contact form messages go to more than one person, ensuring that the message is received and responded to in a reasonable time frame. If a staff member changes jobs or leaves the organization, there is always someone available to answer the contact form messages
- Regularly hire a third party vendor to test the security of the Town's:
    - Internal networks
    - Website
    - Web applications
    - Staff security awareness
    - Physical security of Town data and IT infrastructure
    - Review of policies and procedures affecting the website, data and IT infrastructure security
- The following are corporate best practices and recommended by the security auditors:
    - Run regular, mandatory staff, council and committee security awareness training
    - Development of Policies and Procedures, including regular updates to the:
        - IT Acceptable Use Policy
        - Council IT Usage Policy

      as well as other internal data and security related Policies
    - Regular security training for IT staff
    - Development of internal system security strategies

E. The Blue Mountains Strategic Plan

Goal #4: Promote a Culture of Organizational and Operational Excellence
Objective #4: To Be a Financially Responsible Organization

F. Environmental Impacts

N/A

G. Financial Impact

N/A

H. In consultation with

Ruth Prince, Director of Finance & IT Services
Tim Hendry, Communications & Economic Development Coordinator

I. Public Engagement

The topic of this Staff Report has not been subject to a Public Meeting and/or a Public Information Centre as neither a Public Meeting nor a Public Information Centre are required. Comments regarding this report should be submitted to Cathy Bailey, Manager of Information Technology at support@thebluemountains.ca

J. Attached

N/A

Respectfully Submitted,

Cathy Bailey
Manager of Information Technology

Ruth Prince
Director of Finance and IT Services

For more information, please contact:
Cathy Bailey
support@thebluemountains.ca
519-599-3131 extension 257