MANITOBA PUBLIC INSURANCE

Notice to all Shops

Increased Cyber-Attacks Against the Insurance Industry

Date published: May 22, 2020

> **Disclaimer**: In an effort to raise security awareness amongst the various entities MPI is involved with, MPI is providing the following information for general information purposes only and it does not constitute legal or other professional advice of any kind. You are advised to seek your own specific legal and professional advice regarding any specific issues you encounter. MPI does not warrant or guarantee the quality, accuracy, or completeness of any information provided.

During the COVID-19 pandemic, cyber criminals have been using various techniques to gain access to confidential information, cripple businesses by destabilizing their information systems, hold hostages through ransomware attacks – or all of the above. For example, in the past weeks and months, cyber criminals have used the pandemic to launch a series of phishing attacks to entice email recipients to click links or open attachments within emails.

MPI has learned that cyber criminals are now targeting the insurance industry, both the principal companies and their partners, like yourselves. Those companies have received phishing emails with subjects that relate to denial of claims, delays in payments, and so on.

MPI would like to share the following indictors of compromise (IOC) as an example of what the insurance industry is seeing. The chart below lists some of the email addresses used in these attacks, the email subject lines, the names of infected attachment, and the language used in the body of the emails.

While the example below is a real one, we believe there are many more out there. MPI brokers and partners are encouraged to use the information below to update your various security systems to block such emails.

We ask all MPI brokers and partners to remain vigilant, to alert your users to possible threats, and to apply strong security controls in order to protect Manitobans' personal information to reduce the likelihood of reputational damages and potential financial impacts.

Thank you for your continued support and assistance.

Malware/Phishing IOCs:	
Email Received Time:	May 19, 2020
Email Senders:	• tisin.geressarv9[@]aol[.]com • tumli.calilindelk[@]aol[.]com • eadhere.rirtj[@]aol[.]com • alhwintrugor19917[@]aol[.]com
Email Subjects:	• Hardships with the vehicles insurance plan policy id 47996 • Hardships with the vehicles insurance plan policy No 27042 • Problems with the car insurance policy ID 17761 • Issues with the auto insurance policy No 87852
Email Attachments:	Title: (req|doc|policy)(-|_)?\d{5}\.xls • req_47966.xls • doc_27042.xls • policy17761.xls • doc-87852.xls
Email Content:	"Dear <*colleague name*>. I'm <*First Name Last Name*>. I've contacted you nearly 7 months ago, and you have sold me vehicle insurance. Unluckily, I had a accident last month. Nothing severe, but the automobile is extremely broken. My insurance company explained me that you had not filled the insurance policy properly. Right here I attach my paper work and the insurance policy - could you please take a good look at it and highlight any problems. Without the corrected policy, most likely I would pay the charge for the car on my own. I am looking forward to your instant response."

SHA-256/MD5 Hashes	• 94abcdcabba0f56d5d4c0d7c49ee29f9c83a30c78128e8ef3a84dab2f8d53646 • f9373edcee399d3b59c220a7d5ba3c1e • 7c2addcf8ab2fdae7a8059b258ef1acb9a034d4c70c3896a4f4df6c6dd14f23e • a512339d722dd05d28d3c25a744fb10c • 9a4d821e1560630e659934d02f763347d00b5b326333fc2eeb3a5a3060ef50eb • 55a8e7cfb3d35b89815b93f45e62a457 • 6abbf6f63244941fbc694447495249fdba1b3ad0a143a0c8376a3c14be7109d0 • 515a1097312fdec5fc600900e74d10c7