

MEL CYBER TASK FORCE UPDATE

NEW CYBER EDUCATION SERIES

The MEL Cyber Task Force is launching a **Cyber Education Series** in May to help keep towns cyber safe.

“The Education Series is a do-it-yourself program that will provides 5 case studies that highlight cyber security issues in neighboring towns, how they were affected and what everyone should do to help prevent the risk from occurring again,” said Ed Cooney who heads up the Cyber Task Force.

“The Task Force decided to provide this program because they realized that by sharing some of the real issues that our members have been experiencing it would make them think more about methods for avoidance and encourage further education for their employees,” said Jon Rheinhardt, Chairman of the Cyber Security Committee

One case study will be released each month through a MEL JIF App push notification. If you don't have the free App click [here](#) for details.

The first Case Study #1 is [“Sharing is \(NOT\) Caring”](#) and involves a municipality that has a common shared drive-type of network setup that comes under attack through phishing, clicking on fake links and the deployment of malware. Case Studies will be posted under the [Cyber Risk Control “Resources”](#) tab on the NJMEL.org website when released. Case Study #1 is available now.

The case studies are easy to understand and provide extremely helpful prevention tips that can be used by anyone. The Cyber Task Force recommends that all JIF Commissioners, IT Professionals, Risk Managers and the senior leadership of the member entities (i.e. mayors, council, board, etc.) participate in the program.

“We hope members will have an elevated sense of the cyber threats and gain a sense of initiative to comply with the MEL Cyber Risk Management Program,” added Cooney. “Participating in the series may also have the added benefit of providing supporting evidence to the administration/IT to get new cybersecurity measures approved and included in the budget.”

Ultimately, everyone can benefit from becoming more cyber aware and taking simple steps to change cyber practices to reduce the risk of cyber-attacks both at work and in their everyday lives.

“This is a tool that is intended to be shared with everyone. No one person is immune from attacks,” said Rheinhardt. “Every single person in each organization should be kept aware of potential cyber pitfalls.”

For more information about the MEL Cyber Risk Management Program, contact your Risk Manager, JIF Executive Director or Underwriting Manager.

For details contact your local JIF Safety Director



MEL