the Municipal
RISK MANAGER
A PUBLICATION OF THE MAINE MUNICIPAL ASSOCIATION
APRIL 2024

Several MMA Property & Casualty Pool members have unfortunately been fooled into paying automated clearing house (ACH) payments from fraudulent cyber criminals.

The typical plot utilized by cyber criminals is that they send you an email which resembles that of one of your vendors, and within the email not only request a payment but also advise that they have recently updated or changed their bank accounts, and therefore request that you submit all payments to the new account. It is imperative to note that public and governmental entities are considered soft targets for such attacks, as much of their daily business transactions are publicly disclosed, such as bid awards and requests for proposals. This level of transparency provides criminals with much of the information that they need to assume the identity of your vendor and commit the attack.

A second attack strategy involves direct actions against your employee's banking information. A member of your finance department (again easily determined via a search of your websites contacts) receives an email from the employee requesting a change to their direct deposit bank account. Unknowingly, the receiver doesn't realize that they are being attacked, updates the account details and the money is gone.

In these fast times of electronic communications, we cannot stress enough the importance of implementing safeguards for whenever a banking account change is requested.

- Utilize a written account change form that must be completed by your employees and signed in person.
- Arrange contact logs with all vendors so that you can call a specific phone number and person to verify and document the change request.
- DO NOT respond to the email with the request or use the contact information contained within the email.

The U. S. Cybersecurity & Infrastructure Security Agency (CISA) is issuing strong warnings that every organization—large and small—must be prepared to respond to disruptive cyber incidents. As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, information can be used to render assistance, warn other organizations, and prevent entities from falling victim to a similar attack. For further CISA information, available tools and recommendations please visit: https://www.cisa.gov/shields-up.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA says "Don't take the Bait" on these phishing messages which usually come in the form of an email, text, direct message on social media or a phone call. These messages are often designed to look like they come from a trusted person or organization, to get you to respond.

Stay Safe with Three Simple Tips

1. Recognize

Look for these common signs:

- Urgent or emotionally appealing language, especially messages that claim dire consequences for not responding immediately.
- Requests for personal and financial information.
- Untrusted shortened URLs.
- Incorrect email addresses or links, like amazan.com.

A common sign used to be messages including poor grammar or spelling errors. However, in an era of artificial intelligence (AI) some emails will now be written without mistakes, so look out for the other signs.

2. Resist

If you suspect phishing, resist the temptation to click on links or attachments that seem too good to be true and may be trying to access your personal information. Instead, report it to protect yourself and others. Typically, you'll find options to report near the person's email address or username. You can also report via the "report spam" button in the toolbar or settings.

3. Delete

Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. Just delete.

If a message looks suspicious, it's probably phishing.

However, if you think it could be real, don't click on any link or call any number in the message. Look up another way to contact the company or person directly.

- Go to the company's website and capture their contact information from the verified website. Search for the site in your web browser or type the address yourself if you're sure you know it.
- Use another way to reach the person to confirm whether they contacted you. For example, if you get a strange message from your friend on Facebook, and you have their phone number, text or call them to ask if they sent the message.

The Municipal Risk Manager

The Municipal Risk Manager is published seasonally to inform members of developments in municipal risk management which may be of interest to you in your daily business activities. The information in these articles is general in nature and should not be considered advice for any specific risk management or legal question. You should consult with legal counsel or other qualified professional of your own choice for specific questions.

Publisher: Risk Management Services **Editor:** Marcus Ballou
Layout Design: Sue Bourdon

P.O. Box 9109, Augusta, ME 04332 I 800-590-5583 or (207) 626-5583

FREQUENTLY ASKED QUESTIONS

What is Fraudulent Impersonation & How to Prevent It

Fraudulent impersonation attacks occur when cybercriminals fraudulently pose as members of your business, with the intent of gaining access to funds, stealing data, or harming your operations. Such impersonation attacks are commonly attempted via email communications and routinely contain a sense of urgency prompting you to make a quick and rash decision.

Steps to Improve Cybersecurity

Public entities can reduce cyber threats and mitigate the cost of cyberattacks by implementing these recommended security measures.

- Use multifactor authentication, which grants access to login only after successfully presenting two or more pieces of evidence to authenticate user access.
- Update antivirus programs and use software that includes access to firewalls.
- Use encrypted data storage.
- Implement strong password control measures and change passwords frequently.
- Use predesignated contacts for all bank transaction change requests.
- Update hardware and software packages.
- Provide ongoing employee training on security practices, passwords, phishing identification, and overall cyber security.
- Adopt a rapid response plan that includes the response team, vendor contacts, insurance contacts and notification templates.
- Implement computer use and social media policies.
- Prohibit the use of personal drives and or equipment.
- Verify that daily backups are performed so that data is retrievable.

Property & Casualty Pool Renewal Thank You and Reminder

We would like to thank our members for their continued participation and cooperation in the Property & Casualty renewal application process. Renewal applications were due to be completed by March 29, 2024. For those members that have not yet completed the application, we would like to offer our assistance. If you would like help with your renewal application, please email rmsunderwriting@memun.org or call us at (800) 590-5583.

The continuing success of the Property & Casualty Pool is only made possible through the assistance of our dedicated members. Therefore, the RMS Underwriting Department would like to personally thank our members for their support, understanding and commitment.

MAINE MUNICIPAL ASSOCIATION
RISK MANAGEMENT SERVICES

ONLINE UNIVERSITY & SAFETY MANAGEMENT SYSTEM

Maine Municipal Association is committed to providing participants in our Workers' Compensation Fund and/or Property & Casualty Pool the highest quality educational experience.

We have courses that have been pre-approved for continuing education credits (CEUs) for the Society for Human Resource Management – Certified Professional (SHRM-CP). There are currently 82 courses that have been pre-approved. The education hours will be shown on the employees' certificate of completion if they have added the certification to their profile before taking the training. The certification has already been set up in the system for employees or administrators to add the person profile.

For more information or to become a local administrator, please contact us at 1-800-590-5583, or by email:
rmslosscontrol@memun.org
www.memun.org

Sample of SHRM pre-Approved Courses:

- Discipline and Termination
- EEO Laws
- Hiring Liability
- Lawful Interviewing
- Record Retention
- Family and Medical Leave Act
- Title I & ADA

We also have over 200 courses for managers. This could be for a new supervisor or manager or for an existing manager who is looking for a new skill or a refresher of their skills.

Sample of Management Courses:

- Budgeting
- Dealing with Conflict
- Coaching
- Employee Retention
- HIPAA
- Diversity
- Emotional Intelligence
- Media Training
- PCI Security

Exposures Spring Up

With the arrival of spring, we find that hazardous insects, vegetation and other environmental exposures are also springing back. Unwelcome exposures including ticks, poisonous plants, and our newest friend the brown-tail moth will be hatching and growing soon, but with some simple steps we can work and enjoy the outdoors while being protected.

Simple Precautions to Avoid Contact with Insects and Insect Borne Illness

- Avoid direct contact with ticks and other insects.
- Walk in the center of cleared trails to avoid brushing up against vegetation and don't walk through wooded and brushy areas with tall grass, vegetation and debris.

- Wear light-colored clothing to make ticks easier to detect.
- Tuck your shirt in and long pants into socks or boots to keep ticks on the outside of your clothes. Do not wear open-toed shoes or sandals when in a potential tick habitat.
- Use bug and tick repellents. Remember some repellants need to be reapplied periodically to be effective. When using repellents always follow product directions.

Reduce Hazards Through Property Management

Reduce the humidity on your property, since insects tend to be susceptible to dehydration. You can reduce humidity by pruning trees, clearing brush, removing litter, and mowing grass short and letting it dry thoroughly between watering.

Make your property unattractive to animals that are hosts to ticks by eliminating bird feeders, birdbaths, and salt licks.

- Erect fencing around the property to deter animals.
- Clear away wood, garbage, and leaf piles.
- Remove stonewalls that provide habitats to wildlife.
- Have your property chemically treated. Seek professional advice.

Avoiding Exposures to Hazardous Plants

- Familiarize yourself with the area and what flora you might encounter.
- Never touch plants and then touch your mouth, nose, eyes or any open wounds.

- Keep in mind that even when plants are dormant, they can still cause a rash.
- When in doubt, avoid contact.

More information on bug and plant safety can be found on our web site www.memun.org. Hover over Risk Management and select Toolbox Talks links. Also, members of Risk Management Services programs have access to the Online Safety Training and the Field Biological Hazards course which contains information on ticks and insect bites, as well as poisonous plants.

Potholes Season

WHAT IS THE POTHOLE LAW?

Within the local highway law there is what is commonly referred to as the "Pothole Law." When someone claims their vehicle was damaged because of a pothole or similar road defect, the issue is governed by the "Pothole Law," see 23 MRSA §3651-3655. The Pothole Law requires municipalities to keep town ways (and State roads under municipal control) in good repair.

WHAT IS MY TOWN'S LIABILITY?

The town's liability arises from the physical condition of the road itself, not the town's negligent use of the vehicles or equipment. Three facts must be established before a municipality will be held liable under the Pothole Law:

- First, the defect which caused the damage must be in a town way.
- Second, the damage must be the result of a highway defect.
- Third, the town must have had at least 24 hours prior actual notice of the defect in question and failed to correct it.

RECOMMENDATIONS:

- Have a written plan documenting notice and the date and time of road repair.
- Record and log for at least six months the time and method of repair.
- The statute does not specify what type of repair must be made. The repair will be judged on a reasonableness standard.