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

FRAUDULENT IMPERSONATION ALERT

Risk Management Services has received numerous reports of fraudulent activities related to bank account change requests. If you receive a request to edit or update banking information from anyone, including employees, vendors, and contractors, please stop and review your entity's policies before proceeding. Recently, several members have been spoofed, which is an activity that involves using fake emails, display names, phone numbers, or web addresses to trick people into believing they are communicating with a trusted source. This has led to unauthorized changes in employee or vendor banking information. Therefore, it is critically important to confirm the request by utilizing preapproved communication methods and known contacts. **NEVER REPLY** directly to the initial request as a form of verification. The bad actors are well trained and will reply to appear legitimate and ultimately trap you into sending them your money!

It is important to note that as public-facing entities, much of your information is accessible to the public. This makes it easy for bad actors to identify who works for your entity and their positions. They can also see bid requests and awards, making it easy for them to send emails that appear to be from legitimate contractors. If you are not careful, you could fall into their trap. Therefore, it is crucial to have proper communication arrangements in place to verify requests. Use a designated communication method such as pre-established verification phone numbers or email accounts to confirm the legitimacy of the request and do not reply directly to the initial inquiry. Additional protective measures include:

- **Using Multifactor Authentication (MFA):** Implement MFA for accessing sensitive systems and making changes to account information. This adds an extra layer of security.
- **Educating Employees:** Regularly train employees on recognizing phishing attempts and other fraudulent activities. Awareness is key to prevention.
- **Securing Communication Channels:** Use secure and encrypted communication channels for sharing sensitive information.
- **Monitoring Accounts:** Regularly monitor accounts for unusual activity and set up alerts for any changes to account details.
- **Implementing Strong Policies:** Have clear policies in place for verifying and processing requests for changes to account information. Ensure all employees are familiar with these policies.

- **Conducting Regular Audits:** Conduct regular audits of your security practices and update them as needed to address new threats.

By following these practices, you can significantly reduce the risk of falling victim to fraudulent impersonation. Stay vigilant and proactive so that together we can protect us all.

Strengthening Cybersecurity in Governmental Entities

In today's digital age, governmental entities face increasing risks from cyber threats and data breaches. Safeguarding sensitive information and ensuring continuity of operations is essential, and is achieved through robust cybersecurity measures and adherence to best practices. Public entities of all sizes are encouraged to implement the following key cybersecurity elements:

Written Acceptable Use Policy (AUP): A comprehensive AUP establishes expectations and guidelines for using computer systems within the organization. It outlines permissible activities, defines appropriate behavior, and details the potential consequences for policy violations.

Passwords: Entities should establish requirements for password complexity, length, and regular expiration. Implementing multi-

continued on page 26

Risk Management Services is grateful for your participation in MMA's 88th Annual Convention. Your presence and participation were instrumental in making this event a resounding success.

Our convention was designed to provide valuable educational resources on a variety of critical topics, and we are thrilled that so many members took advantage of these opportunities. With sessions on important topics, such as essential protections for unforeseen threats and discussions on sustainability, the event was packed with insightful presentations and interactive workshops.

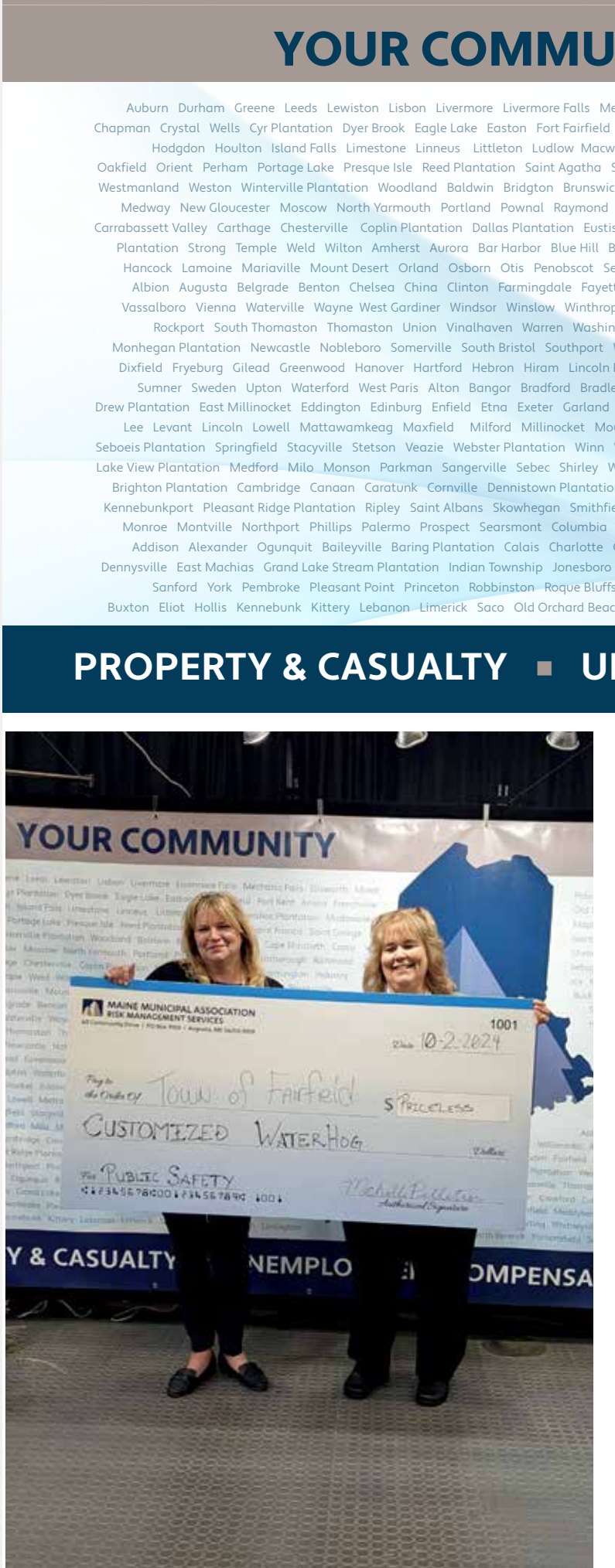
One of the highlights was the session on **SERVESTRONG:** Mental Health Support for Emergency First Responders. The well-being of our first responders is paramount, and it was heartening to see such a strong turnout and active participation in this important discussion. We introduced several online tools and incentive programs aimed at enhancing our communities' resilience and preparedness. Your feedback and enthusiasm for these resources were incredibly encouraging. Additionally, we presented tips and tools to simplify the Workers' Compensation payroll audit process, and we appreciated your participation.

We would also like to thank you for visiting our booth and to congratulate our raffle winners:

The towns of Fairfield, Union, Swanville and Milo are the winners of the personalized Waterhog absorbent mats. The winners of our automobile safety preparedness duffels are Bethany Child of Dixfield, Kylee Coburn of Parkman, Melissa Albert of Eliot, and Andy Hart of Carmel.

We hope that the knowledge and connections you gained during the convention will be beneficial in your professional and personal lives. Your commitment to continuous learning and improvement is what makes our community strong and vibrant.

Thank you once again for your dedication and support of MMA Risk Management Services and we look forward to seeing you at future events and continuing our journey towards safer, more sustainable, and supportive communities.



NITY

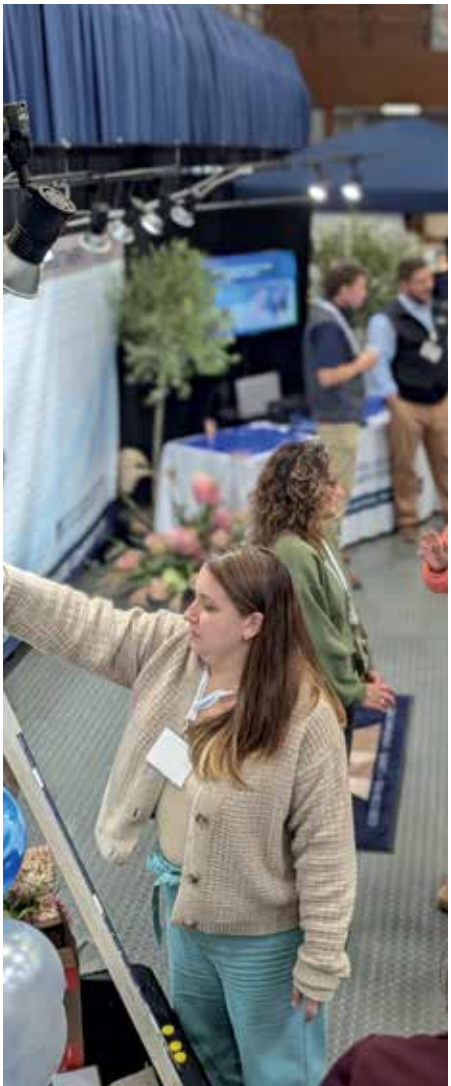
OUR COMMITMENT

echanic Falls Ellsworth Minot
Fort Kent Anson Frenchville
ahoc Plantation Madawaska
Saint Francis Saint George
k Cape Elizabeth Casco
Scarborough Richmond
s Farmington Industry
rooklin Brooksville
dgwick Sorrento
ce Gardiner
o Appleton
gton Alna
Waldoboro
Plantation
ey Brewer
Glenburn
unt Chase
Woodville
Wellington
n Detroit
eld Solon
Searsport
Cherryfield
Jonesport
Talmadge
h Limington

Poland Harpswell Sabattus Turner Wales Allagash Amity Ashland Blaine Bridgewater Caribou Castle Hill Caswell
Old Town Eastport Garfield Plantation Sullivan Glenwood Plantation Grand Isle Hamlin Hammond Haynesville Hersey
Mapleton Mars Hill Masardis Merrill Monticello Moro Plantation Nashville Plantation New Limerick New Sweden
Saint John Plantation Sherman Smyrna Stockholm Van Buren Manchester Wade Wallagrass Washburn Westfield
Chebeague Island Cumberland Falmouth Freeport Frye Island Gorham Gray Harrison Long Island Pittsfield Naples
Sebago Woolwich South Portland Standish Westbrook Windham Yarmouth Woodstock Avon Acton New Canada
Jay Kingfield New Sharon New Vineyard Rangeley Harrington Rangeley Plantation Steuben Sandy River Beals
Bucksport Castine Cranberry Isles Dedham Deer Isle Eastbrook Franklin Frenchboro Gouldsboro Great Pond
Southwest Harbor Stonington Surry Swans Island Tremont Trenton Verona Island Waltham Winter Harbor
Hallowell Litchfield Monmouth Mount Vernon Oakland Pittston Randolph Readfield Unity Rome Sidney
Camden Cushing Friendship Hope Isle Au Haut Matinicus Isle Plantation North Haven Owls Head Rockland
Boothbay Boothbay Harbor Bremen Bristol Damariscotta Dresden Palmyra Edgecomb Jefferson
Westport Island Whitefield Wiscasset Andover Bethel Brownfield Buckfield Byron Canton Denmark
Lovell Mexico Newry Norway Otisfield Oxford Paris Peru Porter Roxbury Rumford Stoneham Stow
Burlington Carmel Carroll Plantation Charleston Chester Clifton Corinna Corinth Dexter Dixmont
Greenbush Hampden Hermon Holden Howland Hudson Kenduskeag LaGrange Norridgewock Lakeville
Newburgh Newport Orono Orrington Passadumkeag Patten Penobscot Indian Nation Plymouth Morrill
Abbot Beaver Cove Bowerbank Brownville Dover-Foxcroft Greenville Lincolnville Guilford Kingsbury Plantation
Willimantic Arrowsic Bath Bowdoin Bowdoinham Georgetown Phippsburg Topsham West Bath Athens Bingham
Embden Fairfield Harmony Hartland Highland Plantation Jackman Madison Mercer Moose River New Portland Beddington
Starks The Forks Plantation West Forks Plantation Belfast Belmont Brooks Burnham Frankfort Freedom Islesboro Jackson Knox Liberty
Stockton Springs Swanville Thorndike Troy Waldo Winterport
Alfred Columbia Falls Cooper Crawford Cutler Danforth Deblois Cornish
Lubec Machias Machiasport Marshfield Meddybemps Milbridge Northfield Dayton
Topsfield Vanceboro Waite Wesley Whiting Whitneyville Arundel Berwick Biddeford
Lyman Newfield Shapleigh North Berwick Parsonsfield South Berwick Waterboro

MAINE MUNICIPAL ASSOCIATION
RISK MANAGEMENT SERVICES

NEMPLOYMENT COMPENSATION ■ WORKERS' COMPENSATION



Strengthening Cybersecurity in Governmental Entities (continued)

factor authentication (MFA) adds an extra layer of security by requiring additional verification beyond just a password.

Backup and Recovery Procedures: In the event of data loss or system failure, having a reliable backup is imperative for restoring operations swiftly and minimizing downtime. Develop written protocols for regular backups of critical systems and data and test these backups periodically to verify their integrity and effectiveness.

Data Privacy and Security Training: Human error remains one of the leading causes of security incidents, underscoring the importance of ongoing education and awareness training for employees. The MMA Online University offers numerous training courses designed to help your team avoid cybersecurity traps.

Prohibition of Unencrypted Protected Data: Sensitive data, such as personally identifiable information (PII), healthcare records, and financial data, must be adequately protected to prevent unauthorized access and comply with regulatory requirements. Entities should strictly prohibit the storage of protected data on removable media.

Remote Access Security Measures: Entities should employ secure methods such as virtual private networks (VPNs), firewall protections, and multi-factor authentication (MFA) to authenticate remote users and encrypt data transmission.

Timely Application of Updates and Patches: Software vulnerabilities represent a common attack vector for cybercriminals seeking to exploit weaknesses in organizational systems. Ensuring timely application of updates and patches is crucial for maintaining security.

Regular System Vulnerability Monitoring: Continuous monitoring for system vulnerabilities is essential for identifying and addressing potential security risks proactively. Prompt remediation of identified vulnerabilities helps mitigate the risk of exploitation by cyber attackers and enhances overall system security.

Physical Security Measures: Physical security is paramount for protecting sensitive data and infrastructure. Ensure that data centers and other critical facilities are located in secure areas accessible only by authorized personnel. Access controls such as keys, swipe cards, and access codes should be strictly managed to prevent unauthorized entry and safeguard against physical threats.

Guest WIFI Access Security: Municipal entities should segregate guest WIFI networks from internal networks and implement access controls to prevent unauthorized access to secure data and resources.

Helpful resources:

CISA- Cybersecurity and Infrastructure Agency
https://www.cisa.gov/

FCC- Federal Communications Center- Model Plan
https://www.fcc.gov/cyberplanner

FEMA- Federal Emergency Management Agency
https://community.fema.gov/ProtectiveActions/s/article/Cyberattack

CIS- Center for Internet Security
https://www.cisecurity.org/

FREQUENTLY ASKED QUESTIONS

WHAT IS TWO-FACTOR AUTHENTICATION?

Two-factor authentication is a simple tool utilized to protect your entity's computer systems from attacks. The tool strengthens access security by requiring two methods to verify a user's identity prior to allowing access. With two-factor authentication, only you can access your account on a trusted device, application or website.

HOW DOES TWO-FACTOR AUTHENTICATION WORK?

Two-factor authentication strengthens access security by requiring two methods (also referred to as factors) to verify your identity. An example of two-factor authentication is utilizing something you know - like a username and password, plus something you have - like a smartphone app to approve authentication requests. Because the username and password alone are no longer enough to access your account, two-factor authentication dramatically improves the security of your devices and the information that you store.

IS THIS REALLY NECESSARY?

YES! As more and more municipalities, governmental entities and utility districts operate virtually and utilize remote storage or offer access to internal services from the outside, robust cybersecurity tools such as two-factor authentication should be implemented and constantly monitored to ensure protection from attackers that may have figured out (or stolen) an account and password.

Many of the attacks you read about in the news most likely could have been prevented if the account had been protected with two-factor authentication. As an example, imagine that you are away from the office vacationing with family when your phone beeps "Allow access?" The two-factor authentication is notifying you that someone is trying to access your account. But because you said "decline" or didn't respond, that person is not able to use your credentials to access your entity's resources.

Two-factor authentication is one of the best ways to protect against remote attacks attempting to access or takeover your accounts. This is simply the next necessary step to protect your data.

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
800-590-5583 or (207) 626-5583