PHISHING ATTEMPTS

We are seeing an increase in phishing attempts specifically with computer hackers spoofing emails from known vendors/contacts advising our members that the vendor's banking information has been changed.

- Before changing any banking information or sending payment to a new financial institution, call a known contact at the other company and verify any banking or financial institution changes from the vendor directly.
- Look closely at the sender's email address. Most times there will be a slight difference in the email address from your known contact. For example, if your known contact's email address is suzyq@hello.org and you receive an email from suzyq@hello.net, you know it is a fake email.

AVOID POP-UPS, UNKNOWN EMAILS, AND LINKS

Never click on any links within an email even if you think it is from a legitimate company that you work with. Instead of clicking a link, go to the company's known website.

Phishing attacks on workers are designed to induce them to open pop-up windows or other harmful links that may contain viruses and malware.

Here's a tip to remember: Never give personal or agency information in response to an email, pop-up webpage, or another type of contact you didn't ask for it. Identity theft is one danger that phishing can cause. It's also how ransomware infections usually occur.

By employing email authentication technology, your agency may assist by preventing these fraudulent emails. You'll generally be notified that the email has been delivered to a quarantine folder, where you can examine whether it's genuine or not.

Be careful. If you're unsure about the legitimacy of an email or other communication, always contact your security department or security lead.

There are third party companies that can help with training on cyber attacks. SDRMA contracts with KnowBe4 to do training and phishing attacks to help train our staff.

ENABLE BEST FIREWALL PROTECTION

The best way to avoid cyber assaults is to use a firewall for the company network. The firewall keeps intruders out of your websites, emails, and other sources of information that may be accessed over the internet. A firewall software installation is also required for someone who uses an agency's website while at work.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is a useful tool for ensuring that only authorized persons access critical information.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Combining biometrics, SMS/text messages, emails, and security questions for the most secure sign-ins. Use additional protection measures such as text validation, email verification, or time-based security codes.

For example, you may allow an employee to access an agency network-maintained device. However, if a user is connecting from an unknown network on an unsecured device, request that they add another layer of protection.

IMPROVE EMPLOYEE AWARENESS OF SECURITY

Employees must be educated on cybersecurity threats to take steps to protect themselves and their agency on a monthly or quarterly basis. There are services that will provide tailored training to employees with updated cybersecurity attacks currently being deployed by cyber criminals.

REGULAR DATA BACKUP

In recent years, the importance of backing up data has grown. Cybercriminals frequently target your data.

- It's critical to back up your files and store them securely, following corporate security standards. Data that is well-protected, encrypted, and regularly updated is critical to safeguard.

- If possible, keep three data back-ups in at least two different locations. Also consider doing back-ups more than one time a day. If you can restore your data from back-ups, it reduces the possibility that you will have to pay ransomware demand.

KEEP HARDWARE UP-TO-DATE

Computer hardware, that the manufacturer no longer supports, may not be able to execute the most recent software security upgrades. Furthermore, older computer equipment makes it harder to react if cyber-attacks occur. Make sure your computer hardware is as up-to-date as possible.

MOBILE DEVICES

Mobile device management (MDM) solutions allows an organization to maintain control of a mobile device in case of theft or accidental loss. With an MDM, you can locate, lock, or remotely destroy any data on the mobile device.

MONITOR THIRD-PARTY CONTROLS

Protecting your data from third parties is an important component of a security plan. A third party has unrestricted access to your information, increasing the risk of insider assaults. It's critical to:

- Keep track of third-party activities to safeguard your data from breaches.
- Limit third-party entry into a certain zone and notify them when they've completed their task so that they can deactivate their access.
- Require vendors to have technology E&O/Cyber Insurance and required the vendor to add you as an additional insured, if possible.
    - What will the vendor do if a data breach occurs?
    - How will they protect your confidential data?
    - Will they cover any losses as a result of their failure to stop a breach?
    - Remember to terminate access to your system by terminated vendors.

SECURE COMPUTERS

Keep your agency's computers safe from prying eyes by preventing access or usage by unauthorized persons. Laptops can be easy targets for theft or loss, so consider securing them when unattended. Create individual user accounts for each employee and requires strong passwords. Only trusted IT experts and key personnel should have administrative privileges.

USE A VPN TO PRIVATIZE YOUR CONNECTIONS

Use a virtual private network (VPN) to secure and privatize your network. It will encrypt your connection and safeguard your sensitive information, even from your internet service provider.

SECURE YOUR WI-FI NETWORKS

Ensure your agency's Wi-Fi network is safe, encrypted, and hidden. Set up your wireless access point or router so it does not broadcast the network name (SSID), revealing your Wi-Fi system's location. Secure access to the router with a password. Train employees not to use a public Wi-Fi as they make it easier to hack into the employee's computer.

CONNECT TO SECURE WI-FI

Secure, encrypted, and hidden networks are what you should seek when working from home. If you're working remotely, a virtual private network (VPN) may be able to help protect your data. When conducting business travel or on vacation, a VPN is essential. Public Wi-Fi hotspots might be insecure and expose your information to being intercepted by strangers. Some VPNs, on the other hand, are safer than others. If your agency uses a VPN that it trusts, be sure you know how to connect to it and use it.

EMPLOY BEST PRACTICES ON PAYMENT CARDS

Collaborate with banks and processors to ensure that the most reputable and validated tools and anti-fraud services are utilized. You may also be subject to additional security standards due to your bank's or processor's agreements. Separate payment systems from less secure apps and don't utilize the same PC to handle payments and browse the web.

LIMIT DATA & INFORMATION ACCESS, RESTRICT AUTHORITY TO INSTALL SOFTWARE

Employees should only be given access to the specific data systems they need for their work, and no software should be installed without permission.

USE A STRONG PASSWORD

Using the same password on numerous sites is like carrying one key around that unlocks your house, car, office, briefcase, and safety deposit box.

If you use the same password for multiple computers, accounts, websites, or other secure systems, keep in mind that all of those computers, accounts, websites and security systems will be as secure as the weakest system on which you have used that password.

We recommend using a password manager that is a service to help generate and store long, unique passwords for all online accounts. They can store PINs, credit card numbers and CVV codes, answers to security questions and more. The password manager will store all of the information with a strong end-to-end encryption.

WHAT DO YOU DO IF A BREACH OCCURS OR YOU RECEIVE A RANSOMEWARE DEMAND

Immediately report a breach and/or ransomware demand to SDRMA. Report any ransomware demand to the FBI's Internet Crime Complaint Center at ic3.gov.

There is a new requirement for cyber incident reporting for critical infrastructure and all public entities within 48 hours of the event. ic3.gov has two links to file an online complaint – Internet Crime Complaint and Ransomware. You will need the following information:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address (this is the person that allegedly committed the internet crime if known)
- Specific details on how you were victimized
- Requested ransom amount and paid (if applicable)
- Overall losses associated with a Ransomware infection
- Email header(s)
- Victim impact statement (ransomware)
- Any other relevant information you believe is necessary to support your complaint