Recommendations

Cyber Incidents Exercise

Recommendations:

Before the attack:

- Have established safety protocols.
- Train all employees on the cyber safety protocols and best practices.
- Be aware. If you are unsure who an email is from, do not respond!
- Double check before you act. Reach out to the sender in person or by telephone to verify the legitimacy of the email if personal information is being requested.
- Protect your personal information. Social engineering can use publicly available information to try to manipulate you into skipping normal security protocols.
- When possible, double your login protection. Enable multi-factor authentication to ensure that the only person who has access to your account is you.
- Shake up your passwords! Use complex passwords and avoid reusing passwords between websites.
- Ensure servers, personal devices, and network appliances are kept up to date with software patches and security updates. Use anti-virus software.
- Ensure that critical systems are regularly backed up.
- Restrict users to the lowest level of access necessary to perform their tasks.

During the attack:

- Contact CSDSIP immediately upon discovery of any cyber breach. Failing to immediately contact CSDSIP can result in diminished coverage.
    - A data breach coach will be in contact to walk you through next steps.

After the attack:

- Retrain employees on safety protocols and best practices.
- Review technological firewalls to ensure optimum protection.
- Revise and implement policies to prevent future cyber incidents.