CYBERATTACK & FRAUD PREVENTION
INFORMATION & RESOURCE GUIDE

Provided by the Office of Indiana State Comptroller Elise Nieshalla, State Treasurer Daniel Elliott & the Indiana Office of Technology

Fraud prevention is crucial to any organization that needs to protect sensitive data, personal information and critical infrastructures from theft, unauthorized access and cyberattacks. Safeguarding your systems against financial loss, lawsuits and operational disruptions does not have to be complicated, but it is necessary. Government entities are being targeted now more than ever -- and we are here to help!

Best Practices for Fraud Prevention

Below is a high-level checklist of reminders to help your office prevent fraud from happening.

- ☑ Conduct routine employee training to help defend against fraud attempts.
- ☑ Review account signers and online banking administrators, and reconcile all bank accounts regularly.
- ☑ Disable banking and other system access immediately when an administrator or other user departs employment.
- ☑ Practice dual authorization for payment practices (one person to create the ACH and second to approve).
- ☑ Implement dual controls when updating payment information (one person contacts the vendor to verify, and second enters the change).
- ☑ Back up all systems regularly and consistently.

Best Practices for Cybersecurity

Below is a high-level list of reminders to help your office prevent a cyber attack from happening.

- ☑ Implement response and recovery procedures to best prepare for various cyber attack scenarios.
- ☑ Create and maintain a Cyber Incident Response Plan -- examples are available at www.in.gov/cybersecurity within the Indiana Privacy Toolkit, Step 6.
- ☑ Establish multi-factor authentication wherever possible to safeguard your most valuable information.
- ☑ Maintain a consistent patching schedule.
- ☑ Identify all of your endpoints that connect to the internet, including cloud access points.
- ☑ Obtain and understand what is and isn't covered in your cyber attack insurance.

More information on the back!

CYBERATTACK & FRAUD PREVENTION
INFORMATION & RESOURCE GUIDE

Indiana Office of Technology (IOT) Resources

We must all work together to protect vital taxpayer services and operations from cybersecurity attacks. The Indiana Office of Technology (IOT) offers a range of resources to help local governments improve their cybersecurity efforts, including:

- Cybersecurity training for local units of government
- Cybersecurity threat notification
- Guidance on building a successful security program available on **www.in.gov/cybersecurity**
- QPAs available to assist in purchasing and securing contractors for hardware, software and telecom
- Virtual town halls on the second Tuesday of each month at 1 p.m. (EST)

Access to all of IOT's local government services at **https://on.in.gov/localgovernment**

Cybertrack is IOT's local government cybersecurity assessment program, which is designed to put local units in contact with top tier experts and provide practical advice. Cybertrack cybersecurity assessments are available for no fee to Indiana local government entities. For more information, visit **incyberattack.org**.

Be Prepared

- Visit **www.in.gov/iot** and click on Local Government Services within the menu, and get familiar with the site. When you experience a cyber attack, you can utilize this site to contact IOT immediately to report your issue while also helping protect others from similar attacks. All information is kept confidential.

- Save the URL to your computer bookmarks and write it down! If you cannot access your computer during a cyber attack, you will appreciate having a hardcopy note to remind you where to report the attack.

- Get to know your vendors, including your banker! Have face-to-face conversations, and often. When an emergency occurs, you will know exactly who to call and they will already be familiar with your process.