


# Cyber Security Best Practices for Local Governments

Last year, a Mississippi municipality—like many other municipalities around the country—suffered from a “ransomware” attack. Hackers took over city computers and locked employees out of their data and email. If the city wanted access to their computers again, the hackers said the city would have to pay a ransom. When this happens, there is little a local government can do to regain access to their system, aside from paying. The ransom might be in the millions. Taxpayers are left holding the bill.

In today’s technical world, information is almost exclusively stored digitally, whether it be on workstations, servers, the cloud, a phone, or any number of storage devices. Hackers have realized there is a benefit for causing harm to organizations like local governments. Your employees’ personal information is likely stored on government computers, along with the personal information of some of your constituents.

Do not fall victim to one of these attacks, open your local government up to lawsuits, and be forced to pay to rebuild your computer network. Here are some of the best practices to ensure that your office’s computers remain protected:

## Device Security

- Change your passwords every 90 days. Passwords should be long and contain a combination of upper and lower case letters, numbers, and special characters such as !, \$, and &;
- Do not write your passwords down and leave them in a place that is easily accessed, like a “sticky note” next to your computer;
- Lock your computer when you are going to be away from it, even if it is just for a minute (on PCs, you can push the button on the keyboard that looks like a Window  and the “L” key at the same time to quickly lock your computer);
- Make sure your computer requires you to login when it starts. This prevents someone from finding your computer and being able to auto login;

## Email Security

- Do not open emails from people you do not know;
  - You can often identify when an email is falsely claiming to be from someone you know by looking at the email address of the sender for spelling mistakes. For example, you receive an email claiming to be from your friend John Doe. When you look closely at the email address of the sender, though, you notice the email misspells John's name. It's spelled jon.doe@yahoo.com. This is a sign someone is pretending to be John. Call John to confirm the email is from him, or just delete the email;
- Do not click links or attachments in emails from people you do not know (this is the number one way hackers get access to your system);
  - You can verify where a link in an email will take you by taking your mouse and hovering over the link. Do not click. You will see the address where the link will take you. If the destination looks suspicious, delete the email. For example, if the email says the link will take you to the White House's website, but the link actually wants to take you to a different site, the email is suspicious. Delete the email immediately;

## Data Security

- Never leave storage devices such as flash drives and external hard drives unattended where they can be stolen;
- Ensure that storage devices such as flash drives and external hard drives are encrypted and require a complex password to access;

## Network Security

- Never provide your computer or email login and password to any website;
- Never share your username, password, or any identifiable information to any person that asks for it;
- Never share any network credentials, such as WIFI passwords, with anyone outside of your organization;
- Never give anyone access to your computer without consent from your organization's technology department. This includes remote access and direct access.

## Continuing Security

- Participate in regular security awareness education and training activities. The Mississippi Department of Information Technology Services provides a list of Security Training opportunities on their website in the “Educating” section of the “Services” tab;
- Consult with an IT professional and adopt computer security policies. Make sure all employees adhere to the policy’s requirements.

Follow these safety tips. Don’t put your office at risk. Don’t put the taxpayers on the hook because you clicked on a bad link. Don’t risk all the data on your computers. Working together, we can protect taxpayer resources and prevent hacking.

Serving Mississippi Together,



State Auditor Shad White

