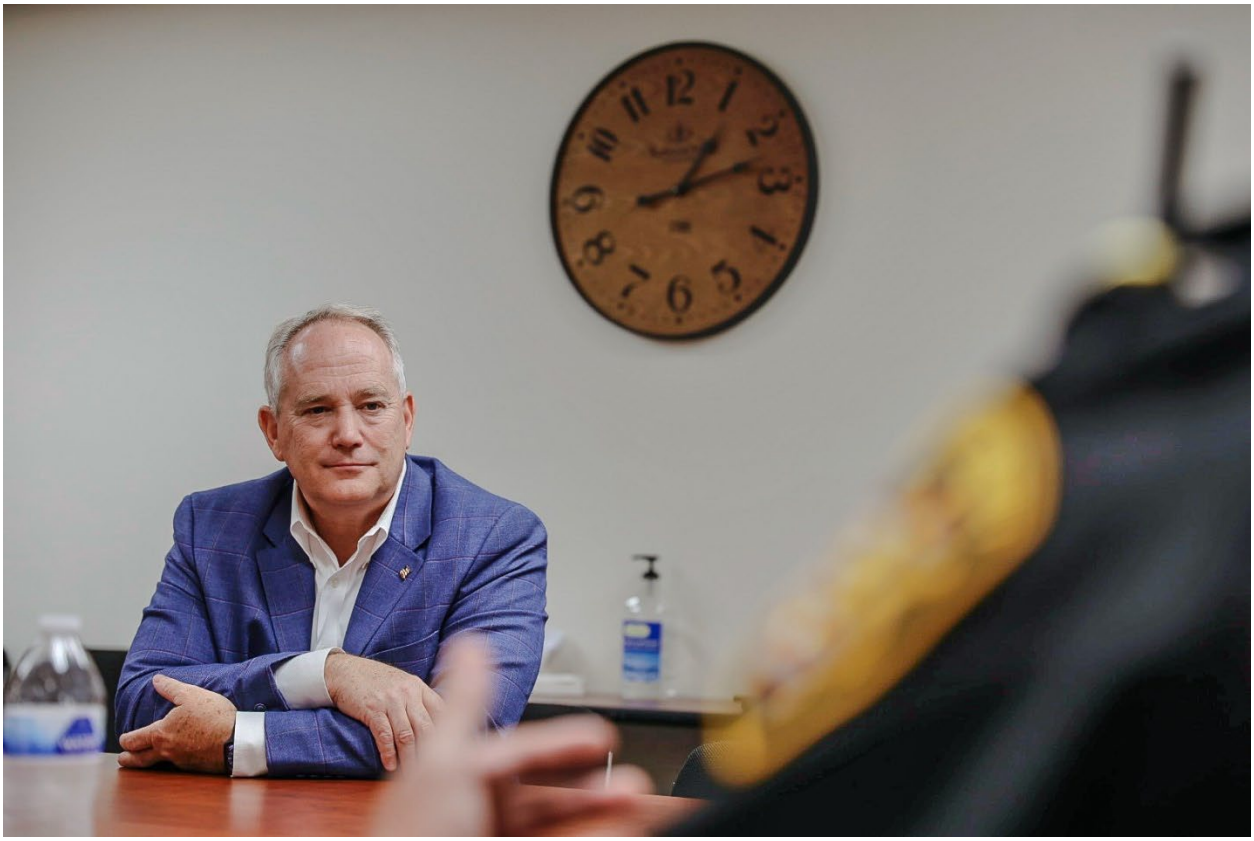
As one of five independently elected statewide offices under Ohio's Constitution, the Auditor of State's office strives for clean, accountable, and efficient governments for the people of Ohio.

With a statewide staff of more than 800 auditors and other professionals, the Auditor of State's office is responsible for auditing all public offices in Ohio — more than 5,900 entities — including cities, counties, villages, townships, schools, state universities, and public libraries as well as all state agencies, boards, and commissions.

The Auditor's office also offers performance auditing for state and local public offices, identifies and investigates fraud in public agencies, provides financial services to local governments, and promotes transparency in government.



Cybersecurity crimes are a challenge for all businesses and governmental entities. Here are some best practices we recommend:

NEVER change the contact or banking information of a vendor or employee without independent verification. In-person communication is always the best practice for verifying identity and contact information. Never use email to verify change requests.

• Require in-person verification whenever possible for requests to change payment information. It is a best practice to also use a second-person verification when the vendor is not personally known by the paying agent, by having the person or department that deals with the vendor personally also verify the identity and confirm the change request.

• If distance prevents in-person verification, use only an independently verified contact person and telephone number. Do not use contact information from the change request; instead, find a phone number from a validated source, such as a prior invoice or a regularly updated employee or vendor contact information listing. Another source for a valid telephone number is the company's known website.

• When using a telephone call to validate the vendor contact or identity of an employee, always ask the employee or vendor a question related to past experiences or conversations that only they would know the answer to.

• Require secondary, internal approval for all payment requests, payment instruction changes, and changes to employee or vendor contact information. The payment change initiation and payment approval functions should be done separately.

Regular backups: Back up the data on your system regularly. If your system becomes infected, you can restore it and avoid paying any fee to release your computer or its data. You should also secure your backup either with an external drive or with a cloud backup provider.

Strong passwords: A strong password is **long** and **uses symbols**, **numbers** and a combination of **upper and lowercase letters**. Consider an easy-to-remember **phrase** such as ILikeMondaysInJuly*for your password. Never write them down on a sticky note and attach it to your computer or screen.

Anti-virus software: Anti-virus programs, anti-malware, and pop-up blockers can help deter cybercriminals. Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.

Up-to-date patches: Make sure application patches for your operating system, software, and firmware are up to date.

Email safety: Do not place personal email addresses on your website. If you need an email address listed, set up a catch-all account such as contact® agency¡com.

Trust and verify: Only download software, especially no-charge software, from sites you know and trust. When possible, verify the integrity of the software through a digital signature downloading.

Unsolicited emails: Scrutinize links contained in emails and do not open attachments included in unsolicited emails. Hover over links to verify the destination matches the link. When in doubt, go to the website itself rather than clicking the link (e.g., go to the official UPS site and type in the tracking number rather than clicking the link in an email.)

No phishing: Use a phishing filter with your web browsers. Many web browsers have them built in or offer them as plug-ins. If your web browser doesn't do this for you, do it yourself.

Macro scripts: Disable macro scripts from files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.

"User Privileged": Avoid using an account with Admin privileges. Always use an account with "User Privileged" access. This helps prevent some (but not all) malware from installing.

Remember: Most companies, banks, agencies, etc., do not request personal information via email.

Please learn more on our website at https://www.ohioauditor.gov/; subscribe to regional newsletters and press releases; or check us out on social media:

- https://x.com/OhioAuditor
- Ohio Auditor of State | Columbus OH | Facebook
- https://www.instagram.com/ohioauditor/
- https://linktr.ee/OHAOS