The Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

Work in local government? Here is cybersecurity advice you can use

No matter your job in local government, you have a role to play

Never connect what might be suspect

Installing software or connecting hardware without your IT department's knowledge or permission can create risks for your government's network. For example, all flash drives should be authorized and encrypted by IT prior to use.

Get tough – passwords must be strong enough

Use a passphrase at least 12 characters long with a combination of numbers, upper and lower case letters, and symbols. Use a unique password for every account. Last, keep these passwords secret and lock your computer when you are away.

Pause and think before you click links

Links or popup boxes can be attempts to lure you into giving cybercriminals access to your government's network. You should: 1) Hover your mouse over links to show and verify the actual destination addresses; 2) Go directly to a website instead of using a link; and/or 3) Ask the sender if the email is legitimate – either in person or by phone, but not by email. If phoning them, use a phone number that is from a source other than the email.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated October 2019

Disclose like a pro

Work with your IT department to ensure you are using encryption methods when transmitting or sharing confidential information — even within your government. Email is not a secure means of communicating confidential information – unless it is properly encrypted. Also, only share the minimum information necessary in fulfilling a data request.

Don't be conned – wait to respond

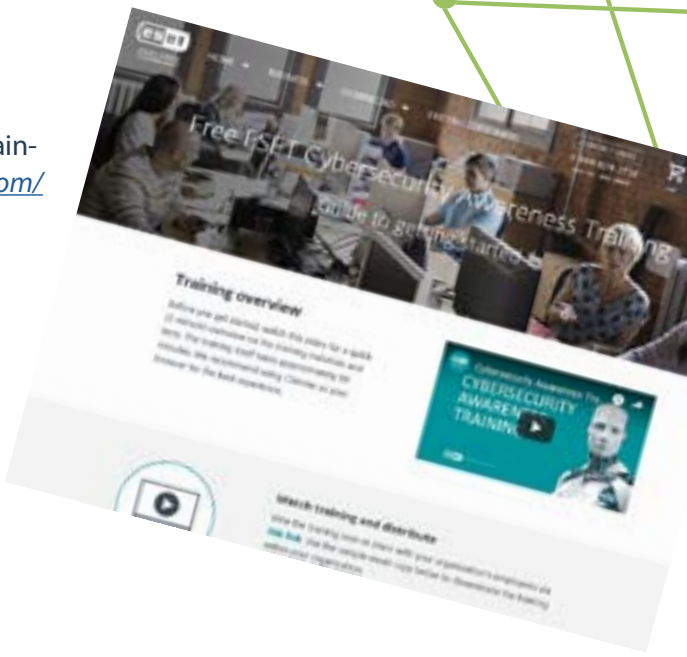
People could misrepresent themselves – and today, you need verification. If a stranger approaches you at work, ask to see their credentials. If they contact you, be sure to verify their identity before you give out information. If they call you, then call them back at their company's headquarters – using a phone number that you obtain from a credible source. If they email you, find a phone number from a credible source- this means a source other than from the questionable email- and speak with them directly to verify the email and if any request is legitimate.

If you suspect deceit – hit delete

You might feel uncertain about an email, even from someone you know — trust your instincts and delete the email. You can always follow up directly with anyone you know to ask them about it, but make sure you do so before taking any action they might be requesting, or opening links or attachments.

Don't refrain; you must train

ESET, a private IT security company, offers a free, 90-minute training that provides a certification upon completion. www.eset.com/us/cybertraining



Disclaimer: Information from ESET is presented for informational purposes and does not represent an official endorsement by the Office of the Washington State Auditor.

CYBERSECURITY
is everyone's job.

Our Office also offers training at conferences on cybersecurity. For upcoming dates and times, visit

sao.wa.gov/Be**CyberSmart**

Center for Government Innovation