A message from Macomb County's Chief Information Officer, Jako VanBlerk:

October is Cybersecurity month and therefore an opportune time to talk about the subject. It's a world-wide phenomenon that creates complex challenges for governments in the digital world we operate in today. Cybersecurity is serious business for everyone, whether you are part of an organization or as an individual; we have arguably never had an enemy as resilient and disruptive as this. It can affect you anywhere, in any capacity, and sometimes with dire consequences. In I.T. we do our best to protect our organization against threads that we sometimes don't even know exist; as individuals we need to do the same.

Information Technology's responsibility to put protections in place to counter Cyber-attacks include:

- Technology and infrastructure needed to defend against targeted threats such as malware, ransomware and phishing
- A comprehensive security policy
- Regular assessments and audits on our environment
- Create awareness in our organization that spans across all Departments by having training through HR's NeoGov system to keep employees informed of what to look out for

A practical reminder on how we can curb one of the most common threads we see today, named "phishing attacks", which usually arrive via email and can appear in many different ways, including:

Suspicious sender's address: The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters to make it look original.

Generic greetings and signature: Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

Spoofed hyperlinks: If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (.com vs .net). Credible banking institutions will never request your ID and password through email.

Spelling and layout: Poor grammar and sentence structure, misspellings and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify and proofread customer correspondence.

Suspicious attachments: An unsolicited email requesting a user to download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

If you see something that looks suspicious or believe that you or your County account has been compromised in any way, please contact the Information Technology Helpdesk at: (586) 469-5697 or helpdesk@macombgov.org and a technology expert will assist you.

Available Training:

Cybersecurity courses are available to you in NEOGOV Learn, including "Cybersecurity Awareness" and "Cybersecurity: Data Privacy and Safe Computing". You can find these optional training opportunities by typing “cybersecurity” in the Course Catalog search bar. For assistance with accessing these courses, please reach out to Training Assistant, Caroline Bronkema at caroline.bronkema@macombgov.org.