# SMALL BUSINESSES

## Protect against ransomware threat today

May 11, 2021

This past week's news of the Colonial Pipeline being shut down in the U.S. due to a ransomware attack highlights the urgency of the threat and need to take action to defend against it. This software attack led to the decision to shut down the pipeline from Texas that is a main source of fuel for the Eastern U.S. The University of Texas at San Antonio's Institute for Economic Development is sharing actions to take to protect your organization.

The threat is real, even for small businesses. "We recognize and appreciate the fact that small businesses comprise the backbone of our nation's economy," said Alejandro Mayorkas, U.S. secretary of homeland security, speaking to a virtual audience of approximately 1,500 small and medium-sized business owners at a May 5th U.S. Chamber of Commerce virtual event. "It is for that very reason that individuals who pose a threat to our nation— who employ cyber tools and particularly ransomware as the vehicle for realizing that threat— target small businesses as extensively as they do."

Fortunately for small businesses, there are cybersecurity resources and best practices available. Victor Malloy, Texas Cybersecurity Compliance Program project manager, at UTSA's Institute for Economic Development leads a cybersecurity training program for small businesses. Malloy has over 20 years of experience as a leader in information technology programs with the U.S. Air Force, Department of Defense, financial services and defense industry, including leading daily cyber operations within the Air Force Cyberspace Operations Center. He provides expert technical guidance on defending against cyber threats.


**"The bottom line is to back up offline, use multi-factor authentication for all users, and validate email links and email attachments."**

"All of us must take actions to protect ourselves from organized attacks like the ransomware incident that has significantly impacted the energy sector," Malloy said. "You can improve your cybersecurity by following the cybersecurity ACES mnemonic."

This cybersecurity ACES mnemonic Malloy refers to is:

**Awareness** – Know that when a cybersecurity incident happens to someone else, it affects all of us, even if you are not someone who uses electronic devices. In the case of this incident the supply of energy resources is causing increases in the cost for all consumers.

**Current Updates** – Make sure you are using the most updated versions of web browsers, email applications, and hardware updates for mobile phones, laptops and electronic devices. Manufactures have a responsibility to design security fixes to products that you purchase for use at home or in business.
**Education** – Learn about proper hygiene in your daily digital habits. Use multifactor authentication to access your mobile phones, laptop and information systems. Keep back-up copies of all your critical files, documents and records for personal information. Follow your organizations information security policies and procedures.
**Stay Vigilant** – If there is something suspicious in a text message, email or phone call, report it immediately to a law enforcement, security official, or leadership in your organization.

Malloy offered an overview on how to mitigate the risk from ransomware attacks on organizations. He said, "The bottom line is to back up offline, use multi-factor authentication for all users, and validate email links and email attachments."

Cybersecurity is also a concern for local, state and national elections. The Institute for Economic Development is currently working with the State of Texas' Department of Information Resources offering cybersecurity and election security training and resources for Texas election officials.

If you are interested in attending the next small business cybersecurity training or learning more about election security training, contact us by calling (210) 458-2458, or emailing: cgc@utsa.edu
Additional Cyber Resources for Small Businesses including a ransomware guide:

**https://www.cisa.gov/ransomware**

**https://www.cisa.gov/cisa-regions**

**https://us-cert.cisa.gov/report**

**https://www.fbi.gov/contact-us**

**https://us-cert.cisa.gov/report-phishing**

South-West Texas Border Small Business Development Center Network
UTSA SBDC Center for Government Contracting

Small Business Development Center COVID Business Recovery Accelerator
South-West Texas Border SBDC Network
UTSA The University of Texas at San Antonio

POWERED BY SBA U.S. Small Business Administration

brought to you at no-cost by CARES Act funding support

UTSA