Tulane cybersecurity expert explains how to avoid becoming a victim of ransomware attacks

August 06, 2021 12:15 PM Roger Dunaway
roger@tulane.edu

Tulane University cybersecurity expert Randy Magiera discusses ransomware attacks in the latest episode of Tulane's On Good Authority podcast. (Photo of Paula Burch-Celentano)

Tulane University cybersecurity expert Randy Magiera discusses ransomware attacks in the latest episode of Tulane's On Good Authority podcast. (Photo of Paula Burch-Celentano)

Taking data hostage is becoming a lucrative business for criminals — and a costly lesson for companies. Last year, ransomware attacks cost U.S. businesses, local government agencies, hospitals, schools and consumers more than $350 million.

Hackers use malicious software to block access to data or a computer system, most often encrypting it until the victim pays a ransom fee to the attacker. The ransom demand usually stipulates a deadline. If the victim decides not to pay in time, they lose the data.

Anyone who uses electronic devices, whether it’s a personal cell phone or computer network that runs a business, is at risk.

Cybersecurity expert Randy Magiera, spoke to Tulane’s On Good Authority podcast about how most people fall victim to ransomware attacks, what to do if you’ve been hacked and the most important steps anyone can take to avoid being scammed.

“My recommendation to consumers is to have a good backup of files in case of a ransomware attack,” said Magiera, an adjunct professor at Tulane School of Professional Advancement. “There are numerous storage device options. Don't just leave stuff on the desktop. For businesses, the most effective control is security awareness training. It seems kind of simple, but the biggest weakness in an organization is an untrained employee.”

Magiera notes there are several ways to protect yourself against ransomware attacks:

- Purchase a high-quality antivirus product. The next-generation antivirus product protects such as Bitdefender, Crowdstrike, Cylane and Sophos are specifically designed to prevent ransomware attacks on your computer, but they are not entirely foolproof.

- Make sure you are browsing safely and not clicking links you do not recognize. Doing this will significantly enhance your protection from ransomware attacks.

- Between a good quality antivirus product, being cautious with sites you visit and avoid opening strange emails, you are protecting your computer against ransomware.

To hear the full discussion, listen below.