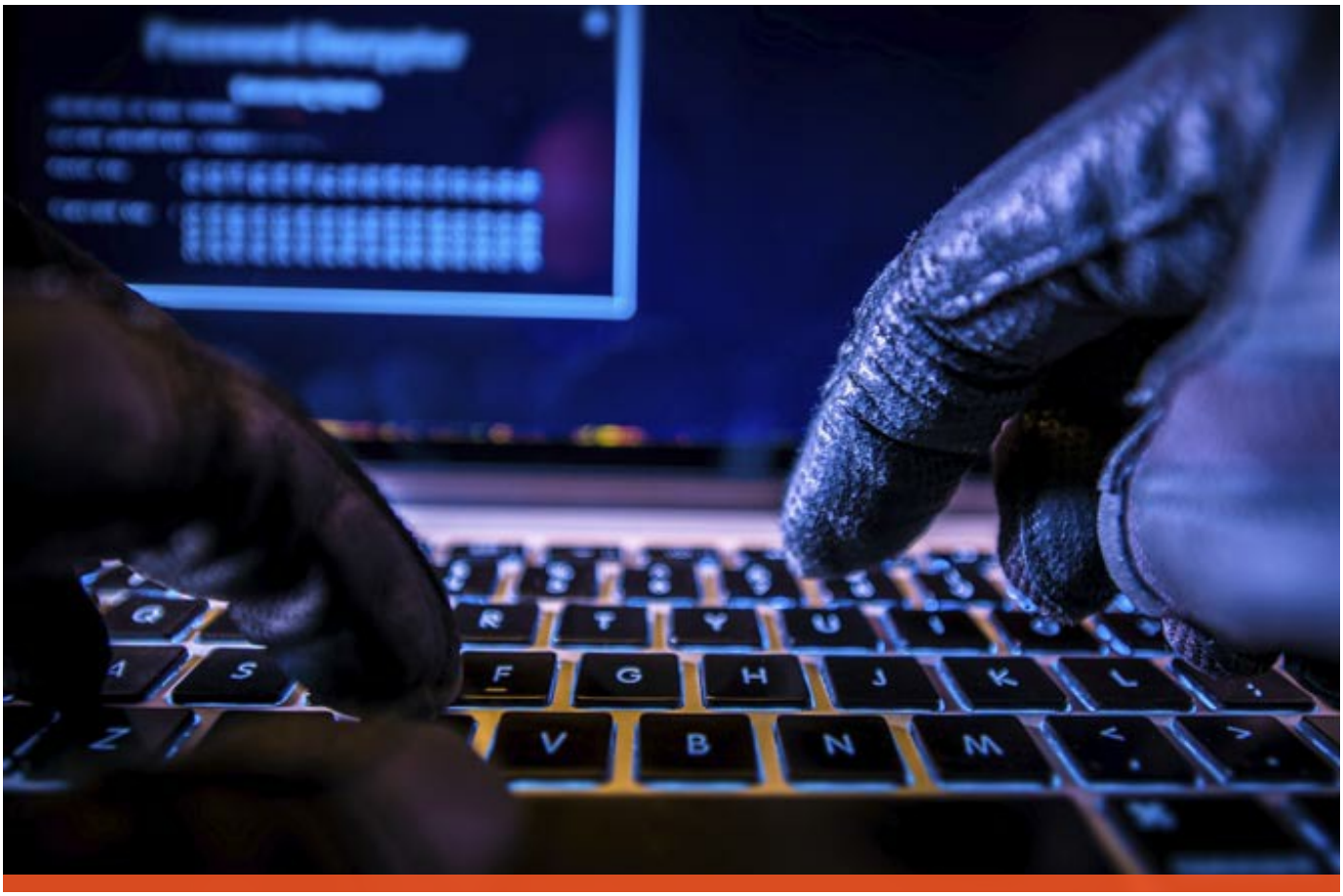
WWJ Cybersecurity Panel At LTU Offers Advice To The 'Pwned'



Colin M. Battersby | Wednesday, October 23, 2019

SOUTHFIELD - Have you been pwned?

Probably. But you're also in good company, according to panelists on a WWJ Leaders & Innovators discussion on cybersecurity, held Thursday morning at Lawrence Technological University.

Using the hacker term for "owned," panelists recommended checking one's email at a website, haveibeenpwned.com, to see whether personal information had been breached in a corporate or institutional data leak.

The bad news—some form of just about everybody's personal information has been leaked. But panelists said there are steps you can take to fix the problem, including simply creating new email accounts. They also recommended regularly changing passwords and using random "pass phrases"—catchy phrases that are easy for users to remember, but hard for others to guess.

"I know it's a pain, I know it's a hassle, but I'm a huge fan of creating specific, individual email addresses for specific functions—an address for banking, and other addresses for other areas of your life," said David Derigiotis, corporate vice president at Burns & Wilcox. "Absolutely, do that." Derigiotis also advised against using one's name in any email address.

Panelists also recommended writing down passwords and keeping that notebook in a secure location. The panel, moderated by WWJ Business Editor Murray Feldman, also advised creating a digital estate plan for

after their passing. Feldman said WWJ would air a segment on digital estate plans soon.

On the corporate side, ransomware is the No. 1 concern. That’s where a hacker gains access to an organization’s database, generally through email, encrypts that data, and then demands ransom to decrypt it.

“There are three options in ransomware,” said Colin M. Battersby, a data privacy and cybersecurity attorney with the Detroit office of the business advisory law firm McDonald Hopkins. “You can start over without your data, which is almost never an option. The other is to restore from your latest backup. The third is to pay the ransom. If you don’t have backup, and you can’t go on without your data, then you’re paying the ransom.”

Most ransomware attacks fly under the radar because the crooks demand relatively modest ransom. But now, victims are beginning to balk at paying higher ransom demands.

Click here to read more from WWJ News - or listen to the recording of the discussion below.

Colin M. Battersby