# IT pros stress education, vigilance, password protection to guard against cyberthreats

**Wayne Risher , USA TODAY NETWORK – Tennessee**Published 1:37 p.m. CT June 30, 2017 | **Updated 1:37 p.m. CT June 30, 2017**

The days of writing computer passwords on sticky notes are long gone.

Cybersecurity is increasingly top of mind as attacks intensify on targets ranging from individuals to small businesses to giants like FedEx.

This week a malicious software temporarily halted trading in FedEx shares while the company cranked out a notice that its Netherlands-based TNT Express subsidiary was among the victims.

Big companies like FedEx that run on information technology have plenty of resources to protect against and recover from such attacks.

But what should individuals and small-business owners do to protect themselves?

**Strong passwords, safe computing**

We turned to Greater Memphis IT Council members and other information technology pros for recommendations.

Here's what the experts said:

Susan Alders, information security officer, City of Memphis:

Strong, long and different passwords for all accounts that are utilized to do transactions over the internet.

Back up data no less than weekly, even on mobile devices.

Load/install anti-virus, anti-spyware, anti-malware on all computing devices, even mobile devices.

Ensure all devices are updated with the latest vendor-provided software patches. (A patch is a software update designed to fix an issue or weakness.)

Alders said citizens can follow the city's Twitter account @Mem_CyberSec to stay aware of cybercrimes and security threats and receive tips to stay safe.

## 'Human firewall' girds business

Drayton Mayers, owner of the Memphis office of technology consulting business TeamLogic IT:

A strong firewall, a strong spam filter and daily updates of anti-virus and anti-malware.

In addition to patching operating systems, make sure operating systems are supported by manufacturers (Microsoft).

“I would create a human firewall inside of my company,” Mayers said. “Every single employee would be trained. They would know what to look for and they would know what to do."

## Training of employees, users is key

Darrell K. Thomas, chairman and chief executive officer, Thomas Consultants Inc.

Don't use public Wi-Fi for personal or business transactions.

Don't store credit card information with any company.

Train employees to spot questionable emails. There is typically something off in the name or content (of dangerous email). “This mistake has been very costly for companies. It doesn't matter how much you spend on prevention equipment, proper employee training is priceless."

Jarrett Morgan, director of information technology, Memphis-Shelby County Airport Authority:

Constant user education and well thought out procedures. “Without question the best defense in fighting cyberthreats is user education. There is no tool, application or hardware solution that can totally protect an organization.”

Third-party cybersecurity assessments to help identify vulnerabilities.

## More on password protection

Paul Murnane, manager of the solutions architects group for cloud services for Mississippi-based C Spire:

Be vigilant about protecting passwords. “Don’t write them down on sticky notes. I know that’s kind of simple, but a lot of people do that."

Make a longer password out of a sentence about something personal, such as children, using both upper and lowercase characters and strategic substitutions: 4 for A, the letter O for zero, L for 1. “You can make passwords that are really long but are easy to remember.”

Use two-factor authentication when it’s an option. In one such scenario, after a user enters a password, a code is text-messaged to the user’s mobile device, and the code is used to complete the login.

“That’s excellent to have,” Murnane said of two-factor authentication. “It’s hard for people to get by that. As long as (the code) is going to your cellphone and you have your cellphone in your possession, there’s typically no way that anybody can beat that.”

## IT council aims to educate

The IT council regularly organizes educational programs on cybersecurity, digital marketing and other topics. "Anatomy of a data breach" was a recent topic of Tech Tuesdays, a lunch-and-learn series at noon the first Tuesday of each month at the Community Foundation of Greater Memphis.

Coming up are Tech 101 on July 28, and Tech 102 in November, co-hosted with the Greater Memphis Chamber’s small business council.

Council Executive Director Regina Whitley said interest has mushroomed, especially among small businesses.

“We started Tech Tuesdays for the purpose of sharing tech trends, especially for small, growing businesses that don’t have full-fledged IT departments. In the 21st-century economy, if you don’t have an IT function you’re challenged to compete in this marketplace.”