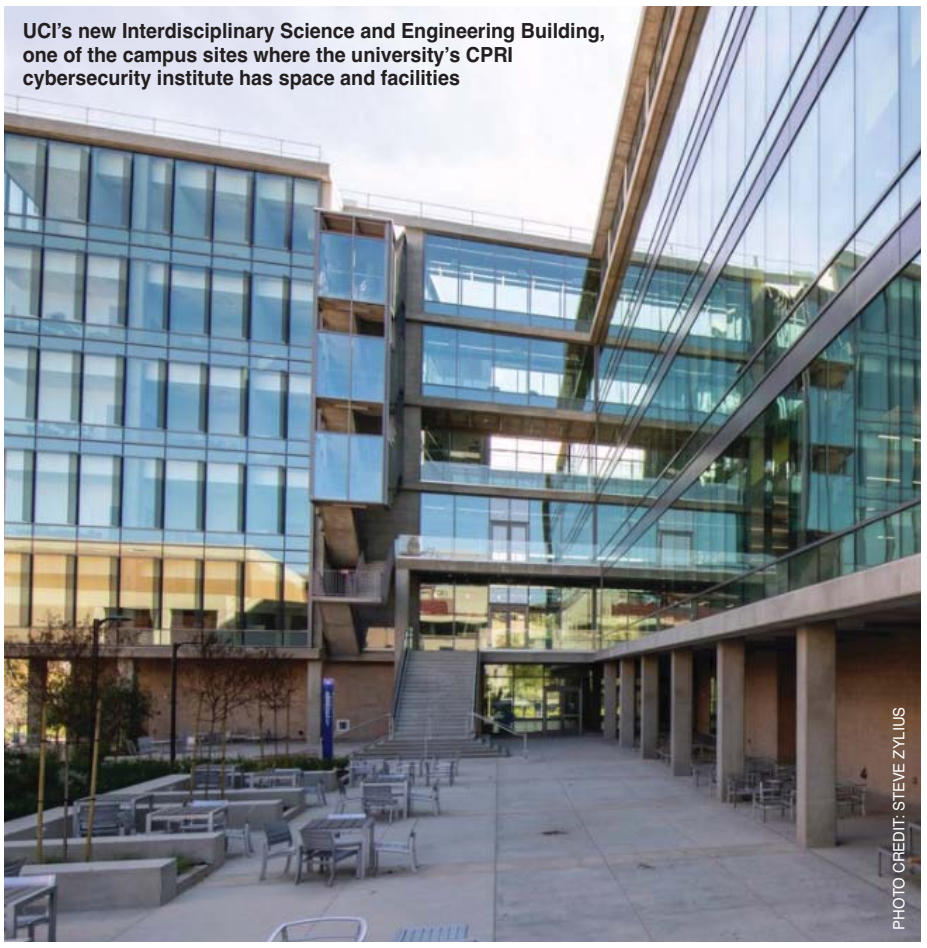
PHOTO CREDIT: STEVE ZYLIUS

UCI's new Interdisciplinary Science and Engineering Building, one of the campus sites where the university's CPRI cybersecurity institute has space and facilities

Computer Tips From UCI's Cybersecurity Institute

Ways to Protect Your Work and Home Computer

■ By KEVIN COSTELLOE

Working from home has become the norm for many firms over the past year and a half; it's also provided a wealth of opportunities for hackers and other criminals to carry out ransomware, corporate espionage, and other forms of havoc on employees and employers who aren't on top of their virtual security game.

While a return to the office will solve some of those problems, other issues remain.


PHOTO CREDIT: UCI WEBSITE

Bryan Cunningham Executive Director UCI Cybersecurity Policy & Research Institute

Bryan Cunningham, the executive director of the **University of California, Irvine**'s multidisciplinary **Cybersecurity Policy & Research Institute**, offers the Business Journal readers his top six cyber self-defense tips for home and work:

1) Multifactor Authentication. Just like your bank, many email and other applications allow you to enable multifactor authentication—usually texting your phone with a numeric code to supplement your user name and password. Enable this everywhere you can. It is both a great defense and can serve as an alert if someone has cracked your password.

2) Biometric Authentication. Wherever possible, enable biometric authentication, usually a fingerprint or photo scan. While not impossible to hack, it is very difficult and far more secure than a weak password.

3) Password Vault or Passphrases. Where you must keep it "old school" with a username and password, either use a complex passphrase (e.g., I Love Hemingway becomes 1LuvH3m$#) or, better yet, secure your passwords in a password manager application such as LastPass or Digital Vault.

4) Ensure End-to-End Email Encryption and Use a Virtual Private Network (VPN). Most major email applications encrypt email sent between users, along with their attachments, though in some cases you'll need to make sure this feature is activated.

Also, consider a VPN to encrypt your communications and searches and mask your true location. Beware, though: VPNs will NOT protect you from being infected with ransomware or other malware if you violate #5, below.

5) Don't Be Stupid. The vast majority of even severe hacks are still caused by people being stupid: e.g., clicking on links from unknown sources; being tricked by phishing emails that appear to be from friends or colleagues; downloading pornography; or giving away personal information via social media "surveys." Don't Do It.

6) Backup, Backup, Backup. There simply is no excuse for any business or person to be crippled by ransomware, when the cure is simply to do a regular backup of all of your data. If you do this regularly, even if you've violated #5, and your data is locked by ransomware purveyors, you can ignore their bitcoin demands, change computers, and download all of your data from your cloud backup..

"Whilst there are no guarantees in life, doing these six simple things is highly likely to protect your privacy and keep you out of trouble at work," Cunningham says. ■

University of California, Irvine's Cybersecurity Policy & Research Institute

UCI Cybersecurity Policy & Research Institute

- **FOUNDED:** 2016
- **EXECUTIVE DIRECTOR:** Bryan Cunningham
- **PARTICIPANTS:** about 550
- **NOTABLE:** 'Don't be stupid' is one of the CPRI executive director's cybersecurity tips