LAMORINDA WEEKLY
Independent, locally owned and operated!
www.lamorindaweekly.com 925-377-0977

Published August 30th, 2023

Council recognizes cybersecurity expert for work with local jurisdictions

By Alison Burns

Orinda Mayor Inga Miller presents Don Hester, from the Homeland Security's Cybersecurity Infrastructure Security Agency (CISA), with a Proclamation of the City of Orinda in Support of Cybersecurity Awareness Month 2023. Photo courtesy City of Orinda

If Don Hester's intention was to terrify his audience, then he probably succeeded. But his recent presentation also served as a timely warning in an ever-evolving cybersecurity landscape where cyberattacks have become increasingly common and sophisticated.

Invited by Douglas Alessio, Orinda's Administrative Services Director, to speak at the Aug. 15 City Council meeting, Hester said his aim was to create a cyber-safe world through education and collaboration.

Hester has over 25 years' experience as a cybersecurity professional and is currently an advisor with the Cybersecurity Infrastructure Security Agency (CISA) for the San Francisco Bay Area. CISA, part of the Department of Homeland Security, is the nation's leading collaborative agency, with a goal to bolster local governments and stakeholders in an effort to make them become more cyber-resilient to attack.

Working at the local government level, Hester says that Oakland, Hayward, Livermore and Modesto cities have all been hit with the kind of cyber incidents that resulted in a debilitating impact on each organization's functions, and prevented critical services from being delivered.

Further afield, perhaps one of the most alarming episodes involved the public school district in New Haven, Conn., which recently lost over $6 million when hackers impersonated the city's chief operating officer. The money, misappropriated via multiple cyberattacks, was long gone by the time the school bus company asked why it had not yet been paid.

And then there are the "ransomware" attacks, of which both Oakland and Hayward have been victims. Even if you have good backups and are able to recover your system, there is still the danger that "the bad guys" discovered documents which they now threaten to put on the "dark web," according to Hester.

One example of this happened earlier this year when over 300,000 confidential school documents, reporting sexual assaults, psychiatric hospitalizations, abusive parents, truancy and suicide attempts, were dumped online by ransomware gangs when Minneapolis Public Schools refused to pay the $1 million ransom.

Sadly, it's not just individual cybercriminals who are responsible for these offenses. Hester knows from experience that "Nation States are oftentimes involved in these attacks."

Since he firmly believes that cyberattacks are not a matter of if, but when, Hester's objective is to assist local governments in better preparing themselves to be resilient. To this end, he is currently working with Alessio in assessing such scenarios. CISA offers cybersecurity courses and a virtual training environment, and staff undertake cyber drills so that they know how to react if confronted with a ransomware situation.

"Better to learn this before, rather than in the middle of, an attack," says Hester.

Although Hester's main focus is geared toward local governments, CISA also strives to educate the public as much as possible and once again are supporting Cybersecurity Awareness Month. Now in its 20th year, Cyber Month is an internationally recognized campaign held every October to inform the public of the importance of cybersecurity.

In keeping with this year's theme, "It's easy to stay safe online," Hester emphasized the "really four important things that stop the bad guys in their tracks."

The first of these, he said, was to turn on multi-factor authentication, contending that your bank account should not just be a username and password. "Somebody gets that and they have access to your full bank account." He also said that it was wise to add this multi-factor authentication to your Facebook account, to dissuade anyone from calling your family to tell them you're in jail and need them to immediately wire you several thousand dollars.

Advice No. 2 was simply to "stop clicking on things."

Third came Hester's absolute conviction that an eight-character password, however complex, can easily be broken. CISA guidance advises using a 16-character password or even installing password management software. Another good idea is to use a passphrase, like a whole sentence.

Finally, Hester said "if you get an email that looks fishy, it probably is. The FBI is not going to send you an email that says they're investigating you for a crime and need to check your computer to prove you're innocent. We want people to understand that there are bad guys out there. Even if you think you don't have anything they want, sometimes they just want to wreak havoc."

Reach the reporter at: info@lamorindaweekly.com

back