LACERA Los Angeles County Employees Retirement Association
300 N. Lake Ave., Pasadena, CA 91101 / PO Box 7060, Pasadena, CA 91109-7060 / www.lacera.com / 626/564-6000

From the Office of the CIO

Ralph Johnson

Chief Information Security Officer

It is time for another weekly Office of the CIO cybersecurity update. We hope you are all well, staying safe and practicing “social distancing”.

Never forget that while working remotely protecting the County’s information remains one of your highest responsibilities.

Zoom for Teleconferencing:

With so many people stuck inside, Zoom has become the default video chat platform. Zoom’s simple, accessible interface makes keeping in touch with family, friends, and coworkers easy to learn and use. At the same time, Zoom has significant privacy and security flaws. As a result, in the past few weeks Zoom has come under scrutiny for several violations of security and privacy including:

- Leaking information to social media
- Susceptibility to eavesdropping (no end to end encryption of communication)
- Local privilege escalation
- Threat actors taking over Zoom sessions and surreptitiously activating cameras.

Do not use Zoom for County work. The County has made significant investment to provide resources for teleconferencing. These include Skype for Business, Teams and Cisco WebEx. These are the tools that you should use for County teleconferencing. If you are having difficulties using these tools, contact your departmental IT support team.

As for the use of Zoom for meetings scheduled by others outside of the County. We understand that County workforce members are often invited to meetings by individuals and groups from outside of the County, some of whom may be using Zoom for teleconferencing. While we do not endorse the use of Zoom for County business, we cannot control the tools that other organizations use. Therefore, it is acceptable to participate in meetings over Zoom scheduled by another party. However, do not install the Zoom client, use the Zoom web client instead. If the content is particularly sensitive, consider rescheduling with another teleconferencing tool.

If you use Zoom for your personal use here is an article that can help you understand how to make its use more secure. View the article from Wired Magazine here.

More Website and Phishing Email Reminders:

We continue to remind you that scammers and malicious actors continue to find even more ways to exploit the COVID-19 crisis. NASA is reporting a doubling of phishing attempts in the last week. ISD also reports an increase attempting to hit County inboxes.

Last week we told you that our partners are reporting that 80% of scams and cyberattacks now are focused on coronavirus themes. We continue to receive warnings from the FBI, DOJ, and other federal and state resources reporting these increases. Some of what is being seen are:

- Phishing scams promising stimulus checks
- Websites promising to provide free Coronavirus vaccines
- Headlines that when clicked distribute malicious software with the ability to bypass antivirus and other protective controls.
- Extortion scams threatening to infect family members with Coronavirus if payment is not made to the threat actors.
- Extortion scams requesting payment for stolen or encrypted files (aka. Ransomware) with a twist in which the scammer claims to possess damaging information obtained from the files about the victim that will be released if the extortion money is not paid.

Be sure to only read online information related to COVID-19 from trusted sources such as legitimate news and publication sites.

Dangerous Websites

This week we do not have any additional dangerous websites to report. However, we will continue to remind you of the ones we have posted in past weeks. Previously we reported the following:

- corona-virus-map[.]com – This is a fake coronavirus map that will install a virus to your computer.
- coronavirusapp[.]site – This site hosts a malicious Android app that purports to track coronavirus activity. The app actually deploys a version of Ransomware to the mobile device.'
- westminsterhj[.]com/OneNote/office[.]php – This is a phishing domain that will attempt to steal login credentials (username and password) This week we have become aware of the following additional websites that you should avoid.

As we identify and validate other sites and threats, we will provide you with appropriate information. Remember when surfing the Internet, be sure you are visiting trusted sites.

Phishing

We will continue to remind you again about the dangers of "Phishing" and how to avoid them. We continue to receive reports form our partners that phishing emails are on the increase. Be sure to exercise caution when opening emails. Again, here are some tips that can help to recognize malicious emails:

- Be very suspicious of emails from unfamiliar people or organizations.
- Watch for a sense of urgency in the message. If the messages is demanding immediate action consider that it may be phishing.
- Never respond to requests for personal information. Those asking for your name, phone number, social security number, credit card, login credentials, etc.
- Spelling and/or grammatical errors are often indicators of phishing. Rarely do legitimate e-mail messages contain these types of mistakes.
- Look at the email address If something looks suspicious, report it.
- Hover over any embedded links or buttons. Examine the web address that appears. If it looks unrelated to the sender or the intended destination DO NOT CLICK ON IT. For example, a .ru destination is Russian, .jp is Japan, .br is Brazil, etc.). See how this works by holding your cursor over this LINK Notice that you will see a dialog box showing you that clicking on it will result in opening the browser to the LA County Website.
- Watch out for unexpected attachments. If you are not expecting an email with an attachment, check with the sender (if you actually know the sender).

Inform your family and friends of these indicators so that they can also be diligent in their email communications.

Securing Your Home Network:

We discovered a nice little video that might provide you with some insights into how to better secure your home. You can view the "Creating a Cybersecure Home" video here.

One of the most important items pointed out in the video is that of securing your home WiFi network. This includes securing the router (i.e. password protect the router access) and ensuring that only trusted devices are connected. If you have any questions about securing your home WIFI network, contact your service provider.

Protecting Our Children:

Not related to your working life but many of you also have children spending more time at home and on the Internet. We found a helpful video that can provide you with some insight into protecting them while they are online. View the video "Protecting Your Kids Online" here.

Where to Report Issues:

Any potential loss, theft, fraud, or compromise, whether suspected or confirmed, or loss of County equipment must be immediately reported to your supervisor and IT Security staff. Report such circumstances to:

- Phish Alert Button (PAB): On County owned computers the PAB is used to report suspicious phishing emails. The PAB is available in the Outlook client, Outlook web browser, and Outlook mobile app.
- Your department's IT Security staff: Follow your departmental reporting protocol, generally the help desk.
- County's Chief Information Security Officer: rjohnson@cio.lacounty.gov or 213-263-5660
- County's Chief Privacy Officer at privacy@ceo.lacounty.gov or 213-974-2164

If you suspect criminal activity against you or a family member you can report the circumstances to:

- An FBI local field office. Field offices can be found at fbi.gov/contact-us/field.
- FBI Cyber Watch at 855-292-3937 or cywatch@fbi.gov.
- Cybercrime Support Network (CSN) at fraudsupport.org.
- Internet Crime Complaint Center (IC3) at ic3.gov. IC3 reports are forwarded to the FBI, Secret Service and Homeland Security. However, the report form is complicated and difficult to complete. Reporting to CSN is easier to complete and forwards the submission to IC3.