From the Office of the CIO

Ralph Johnson
Chief Information Security Officer

April 29, 2020

As this crisis lasts, we will continue to provide these messages to you. However, we will try to make them a bit more targeted and maybe even shorter.

Working from Home (Teleworking):

Working from home has quickly become a common trend due to the current health crisis. Thanks to our friends at the Department of Public Works, the attached .pdf file will help you learn how to better maintain the security of employee, customer, and organizational data while working remotely.

- Taking Security Home Working Remotely.pdf

Cyber-Attacks to Watch Out For:

We continue to receive warnings from the FBI, DOJ, and other federal and state resources reporting increases in attacks.

We have learned about a particularly interesting new attack. Those of you that use Skype (not Skype ofr Business, which is a County provided collaboration/communication tool) to stay connected with family and friends should watch out for this one. This is a Phishing attack that begins with an email that looks similar to a legitimate Skype notification alert. The email indicates that there are 13 pending Skype notifications that can be checked by clicking a “Review” button. Skype generally does not send such notifications via email but through other notification mechanisms. If the “Review” button is clicked the user is directed to a webpage that looks similar to a Skype login page. If the intended victim attempts to authenticate (provide username and password), authentication fails, and their login name and password are captured by the perpetrator.

Again, a reminder of other attacks that have been seen:

- 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.
- Coronavirus-themed spam and phishing messages spreading malware, impersonating the "Centers for Disease Control & Prevention" or the "World Health Organization" (WHO).
- Targeted e-mail addresses to deliver a Word document embedded with a script ultimately resulting a malware infection of the computer
- Malicious coronavirus map hiding malware that steals information from your system(s) etc.

This list has not grown since last week because there are no new schemes. But remember that the malicious among us will continue to devise new and creative ways to compromise our systems, steal our data and exploit our good natures. Be sure to only read online information related to COVID-19 from trusted sources such as legitimate news and publication sites.

Tips for a Safer Home Network:

Adjust Factory-Default Configurations on Hardware and Change Default Passwords: Passwords are a common form of authentication and are often the only barrier between cybercriminals and your personal information. Some Internet-enabled devices are configured with default passwords to simplify setup. But did you know those passwords can easily be found online? To better secure your digital devices it's important to change the factory- default password. Be sure to replace it with a strong and unique password or passphrase for each device.

Secure your Wi-Fi Network with Encryption: Your home's wireless router is the primary entrance for cybercriminals to access your connected devices. To enhance your defenses, use Wi-Fi Protected Access 3 (WPA3) if it is available on your router (use WPA2 if it is not). WPA3 is currently the strongest form of encryption for Wi-Fi. Other methods are outdated and more vulnerable to exploitation.

Double Your Login Protection: Enable multi-factor authentication (MFA) to ensure that only the person who has access to your account is you. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token. For instance, with an iPhone you can utilize your screen lock feature with a pin or password.

Disable Location Services and Remote Connectivity: Location services can allow anyone to see where you are at any time. Consider disabling this feature when you are not using your device. This will further secure your private information. Additionally, most mobile devices are equipped with wireless technologies such as Bluetooth that can be used to connect to other devices or computers. Consider disabling these features when not in use as well!

Safeguard Against Eavesdropping: Disconnect digital assistants, such as your Amazon Alexa, when not in use. Limit conversation near baby monitors, audio recordable toys, and digital assistants. Be sure to cover cameras on toys, laptops, and monitoring devices when they are not in use.

Don't Broadcast Your Wi-Fi Network Name: To prevent outsiders from easily accessing your network, avoid publicizing your Wi-Fi network name, or service set identifier (SSID). All Wi-Fi routers allow users to disable broadcasting their device's SSID. Doing so will make it more difficult for attackers to find a

network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

Install a Network Firewall: Install a firewall at the boundary of your home network to defend against external threats. A firewall can block malicious traffic from entering your home network and alert you to potentially dangerous activity. Most wireless routers come with a configurable, built-in network firewall that includes features such as access controls, web-filtering, and denial-of-service (DoS) defenses, that you can tailor to fit your networking environment. Keep in mind that some firewall features, including the firewall itself, may be turned off by default. Ensuring that your firewall is on and all the settings are properly configured will strengthen the security of your home network.

> **Note:** Your internet service provider (ISP) should be able to help you determine whether your firewall has the most appropriate settings for your particular equipment and environment.

Install Firewalls on Computers, Laptops and Tablets: In addition to a network firewall, consider installing a firewall on all computers connected to your network. Often referred to as host or software-based, these firewalls inspect and filter a computer's inbound and outbound network traffic based on a predetermined policy or set of rules. Modern operating systems come with a built-in, customizable, and feature-rich firewall. Additionally, most vendors bundle their antivirus software with additional security features such as parental controls, email protection, and malicious website blocking.

Remove Unnecessary Services and Software and Install Antivirus Software: Disable all unnecessary services to reduce the potential attack points within your network and on devices, including your router. Unused or unwanted services and software can create security holes on a device's system, which could lead to increased points of attack of your network environment. Additionally, a reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware, such as viruses, worms, and ransomware. Many antivirus solutions are extremely easy to install and intuitive to use, allowing for automatic virus definition updates to ensure maximum protection against the latest threats.

Update and Patch Regularly: Manufacturers will issue updates as they discover vulnerabilities in their products. The perfect example being all of the update notifications you receive on your iPhone! Configuring your device to receive automatic updates makes this easier for many devices, such as computers, phones, tablets, and other smart devices. However, if you need to manually update your device, make sure you are only applying updates directly from the manufacturer (i.e. Apple), as third-party sites and applications are unreliable and can result in an infected device.

Watch out for Phishing:

Continuing to remind you about the dangers of "Phishing" and how to avoid them. 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.).
- 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.

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.
- Auditor/Controller's Fraud Hotline: website fraud.lacounty.gov, telephone 800-544-6861 or email fraud@auditor.lacounty.gov.
- 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.

"Change is hard for the unready." – *Cy Wakeman*