JULY/AUGUST 2021

THE DOWNLOAD

INFORMATION TECHNOLOGY UPDATES FOR EHSD STAFF

What Your IT Team is Working On

- **Windows 1909 Version Update –** IT is continuing to update EHSD's computers. Similar to a visit from Santa, updates happen when nobody sees –during weekend hours. We do notify building managers and supervisors about the dates and times. On the following Monday, technicians are on site to make sure the computers are working as expected. So far, IT updated 643 computers. Next in line is computer equipment for CSB and First 5.
- **Application Development –** Improving communication and timely service is the goal of a new online software application that IT is working on with Personnel. The new app will enable you to send questions and service requests in real-time to Personnel, as well as track the status of inquiries.
- **Equipment Return –** In the next month, EHSD IT will be collecting work-from-home equipment from staff members who have returned to the office full time. We are arranging to use buildings throughout the county as drop-off locations, making this effort as efficient and convenient as possible for everyone involved.

Cyber Security

Following two phishing attacks during June, we want to remind everyone that we are set up to secure impacted PCs and data. However, the best line of defense is all of you as staff members.

Proper email security can protect sensitive information in email communications, prevent phishing attacks, spear phishing and email spoofing and defend against unauthorized access, loss or compromise of one or more email addresses.

A few ways to protect yourself and EHSD from phishing and other types of attacks:

- Only open emails from people you know or can identify.
- Be wary of opening any link or attachment on an email.
- Never give out your username, password or personal information, in an email or on the phone; EHSD will never request that information in an email.
- If you suspect you have replied to a phishing email, opened an attachment or clicked on a link, call the Help Desk immediately with the email description and as much detail as possible. Getting this information to IT is critical.
- Forward the original suspicious email to IT *before* clicking on Phish alert so there can be an immediate response.
- Call the Help Desk if you entered personal information, including passwords, on a form from an unfamiliar source.

Email security is important because malicious email is a popular medium for spreading ransomware, spyware, worms, different types of malware, social engineering attacks like phishing or spear phishing emails and other cyber threats.

Testing, Testing

With power outages being a real possibility over the next few months, testing on Windows Virtual Desktop (WVD) is a priority for EHSD IT. Our thanks to all the current and new testers for their support and efforts.

Workforce Services and EHSD IT are working together to create a way to allow a worker and client to virtually meet through video conferencing. The worker calls into the same Teams meeting with the client, but uses inContact for the audio portion. We capture the voice attestation/signature through Telephonic Signature recording. Staff Development is putting the final touches on the training for workers to learn video conferencing.

Continued on next page

THE DOWNLOAD

INFORMATION TECHNOLOGY UPDATES FOR EHSD STAFF

Continued from page 1

In-Office Worker Tips:

Lock your computer if you step away from your desk. Security of your work computer and the county network is critically important. To easily prevent security breaches, press Windows + L to lock your system right away, then enter your password to log in again. Also, NEVER write down your password or post it in your work area where someone else may see it.

Remote Worker Tips:

Enable two-factor authentication and use an authenticator application:

Two-factor authentication is a method granting access only after you successfully present two pieces of evidence to an authentication mechanism. Two-factor authentication can dramatically reduce the risk of successful phishing emails and malware infections because even if an attacker gets your password, login is not possible without the second piece of evidence. To successfully login, the attacker would need access to whatever is generating your one-time code, which should be an authenticator app or security key. The first and most common evidence is a password. The second takes many forms, but is typically a one-time code or push notification.

Separate work and personal devices:

It might be easier said than done, but it's important to carve out boundaries between your work life and home life, especially while working from home. While it may seem cumbersome to constantly switch between devices for simple tasks, do your best to keep your work computer, home computer, and mobile device activities separate. This can help reduce the amount of sensitive data exposed if your personal device or work device is compromised.

If we missed a topic or there is one you would like us to cover, email Kathy Gaughen at kgaughen@ehsd.cccounty.us.

Contra Costa County
Employment & Human Services
Building Brighter Futures Together