CYBER SECURITY SPECIAL EDITION

PHXCONNECT

The Weekly Connection Newsletter for City of Phoenix Employees • September 26, 2018

FROM THE CITY MANAGER

Dear Employees,

Our lives at work and home are consumed with emails, text messages, electronic calendars, social media connections, bank account apps and Siri and Alexa.

Keeping our technology safe is the responsibility of all of us. Cyberattacks are becoming more sophisticated and it's critical that we are all aware of what to look for and how to react when we think we have seen something fraudulent related to our digital communication.

You will *never* be asked to provide personal information, passwords, or financial information by an email from the city manager, city management or department management. *Always* check before sending or responding to anything that seems out of place.

Please take the time to review some of the safety tips our experts in the city's Information Technology Services Department are providing to us in this special edition of the employee newsletter.

Be informed and be vigilant!

~Ed

KEEP IT PERSONAL

Your personal information is worth a lot of money to legitimate businesses and the bad guys. One wants to know more about you to sell you more goods and services. The other just wants to steal from you. Take these steps to protect your valuable personal information:

- Don't fill out entire profile on your social media pages. The more you share online, the easier it is for someone to get their hands on those details.
- Take precautions when sharing your Social Security number, even the last four digits. Unless it's your bank, a credit bureau or a company doing a background check on you, don't be too liberal with sharing that information. Even those last four digits can provide enough details about you for the bad guys to use.
- Set up a Google alert for your name. This is a simple way to keep an eye on anything someone might be saying about you on the web.
- Keep your social network activity private. Check your privacy settings for all your social media accounts.

⇒ *Tips from: Sandra Stouffer*

⇒ *Telecommunications Services Assistant*

⇒ *Active on social media & shopping sites*

PLAYGROUND FOR HACKERS

Online video games are popular with kids. But did you know most have some type of social component built in, such as direct messaging or chat? To lure kids and take advantage of their trust, cyber thieves use these tricks:

- Pop-up ads or chat links offering free coins, avatars, skins and upgrades can take a player to a website that requires them to download an executable file, which infects the computer with malware designed to steal data.
- Fake login schemes use pop-ups within the game to tell the player they must provide their username and password to continue. The pop-up may claim the site is "under maintenance" as a social engineering ploy to steal a player's account and lock them out.

- Hackers send spam and fake ads to millions of players, asking them to visit websites for free stuff. The botnet is designed to run a fraudulent ad scheme, which relies on more views and clicks to make the hackers money.

Here are some tips to help your child avoid phishing scams on video games:

- If the game allows, set your child's chat options to "friends only."
- Teach your child the "no free lunches" lesson. Emphasize to them that if it sounds too good to be true, it probably is.

⇒ *Tips from: Suzanne Wang*

⇒ *Interim Project Portfolio Manager*

⇒ *Mother of two kids*

SAFETY WITH PUBLIC WIFI

ITS will soon be launching a secure and dedicated Wi-Fi network for city employees to use while working in city facilities. This secure and dedicated Wi-Fi allows city employees to easily access their files and work remotely within city facilities while using their city-owned laptops and tablets.

This project helps protect city employees and city information from the possible dangers of using public Wi-Fi. But here's a few simple security steps to take when using public Wi-Fi with either work or personal devices:

- Turn off your mobile device's Wi-Fi connection when not in use and don't setup your smartphone to automatically connect to any public Wi-Fi.
- Hackers will set up their own hotspots in busy areas. Always ask someone who works at the location for connection details to ensure a legitimate network.
- Paid Wi-Fi doesn't mean safe Wi-Fi; nearly all public Wi-Fi is completely open and completely insecure. There's no encryption to stop anyone from eavesdropping on what you share using public Wi-Fi.
- Change your passwords frequently (at least once every six months) and make sure to use complex passwords.

Buy a VPN and use it on all your devices! A VPN is the best protection you can use if you're going to use public Wi-Fi on any of your devices.

⇒ *Tips from: Chris Barber*

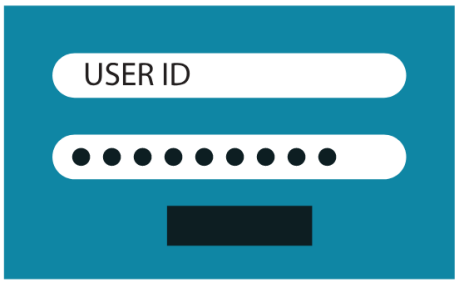
⇒ *Sr. Enterprise Network Engineer*

⇒ *Working on launch of dedicated city Wi-Fi*

AVOIDING CYBER ATTACKS

In the following months, ITS will be implementing a number of improved security features to further safeguard the city from cyberattacks. ITS is working on several projects including a multi-factor authentication, which requires more than one method of authenticating employees' credentials and an upgrade to Windows 10 to take advantage of security updates.

Here are some cybersecurity tips for employees to remember to strengthen the city's resiliency to such malicious attacks.



- Create strong passwords. Never use your name, names of pets or anything that can be easily associated to you. Use symbols and a combination of upper-and lowercase letters.
- Lock up your devices when you leave for lunch, a break or home.
- Be aware of phishing emails. Double check that the sender's email address is recognizable; look for blatant misspellings and grammar; contact the sender directly for verification before responding to any link.
- Don't install unauthorized software. It may put your computer and the city's networks at risk.
- Watch out for fake URLs or websites. These sites will appear to be familiar, but will contain slightly deviated details such as small typos or unusually placed symbols. These variations give you a clue that it is not the real site.

⇒ *Tips from: Walter Davis*

⇒ *Sr. Information Technology Systems Specialist*

⇒ *Working on his Master's degree in law*

PHONE SCAMMERS

The city is in the middle of a multi-million dollar project to replace its aging telephone and network system. The project started in January, and to date, ITS has deployed 3,700 phones in 113 city facilities. The project should be completed by mid-2019, with a total of 11,000 new phones to be deployed to replace the relics from the 80s!

And speaking of phones, here are some tips on how to deal with phone scammers:

- Do not confirm or deny your identity until you know who is calling.
- Decide how to proceed depending on your comfort level after getting the information.
- Check the legitimacy of any agency, organization or company calling you cold by doing a quick online search while on the phone.
- Do not disclose personal information or passwords.
- Ask what the caller wants early in the call.

⇒ *Tips from: Mark Haskin*

⇒ *Project Manager*

⇒ *Assigned to telephone and network replacement project*

If an E-mail looks wrong, send it to:

SpamBusters@Phoenix.gov

If you are having computer issues, call the Help Desk:

534-4357

GET READY TO GROW

Discovering how to pick a perfect fruit tree for your yard can be perplexing! Arizona is ripe for growing all sorts of fruit trees like peaches, apples, apricots, plums, pears, citrus and more.

The Green Garden Group & The Green Team invites you to meet Greg Peterson on **So, You want to Grow a Fruit Tree?** Farmer Greg will walk you through the three things to know about growing fruit trees in your yard. **Details:**

- Tuesday, Oct. 2 at noon
- Calvin C. Goode Building, 10 East
- Receive diversity credits for attending

HELP KIDS WITH CSFD

Help kids learn by creating flash cards with either sight words or basic math facts. You can earn credits towards your department's CSFD goals by giving your time. **Details:**

- Thursday, Sept. 27
- 11 a.m. - 1:30 p.m.
- City Hall Assembly Rooms

Have an idea for the next PHXConnect?
E-mail us: phxconnect@phoenix.gov

JOB OF THE WEEK

Featured Listing: Courtroom Specialist, Municipal Court ($15.51 - $22.65/hour)

"Provides assistance to the Judges and Hearing Officers in the courtroom by performing court-related clerical work and coordinating the flow of court cases and hearings. Available assignments include: Arraignments Section & Courtroom Operations Section –interacts with defendants, attorneys, witnesses, victims, jurors, and police officers, while processing judicial orders; and Jail Court Section –provides assistance to Judges in the jail courtroom and interacts with in-custody defendants, attorneys, victims, police officers, and detention officers, in a jail setting while processing judicial orders. Requires clerical experience in a court or law-office setting. Knowledge of Municipal Court procedures and legal and court terminology is preferred. Apply by Oct. 9."

Each Monday, the city posts jobs available for current employees to consider. Here's the link to the most recent job opportunities.

LEAVE DONATIONS

The following employees are accepting leave donations. If you'd like to help, use eChris to make your donation:

- Miriam Marguliz, senior center assistant, Human Services
- Alycia Colcord, senior human resources analyst, Parks and Recreation
- Maribel Lowe, park ranger II, Parks and Recreation
- Lici Gloria, equipment operator II*gangmower, Parks and Recreation
- Mary Brown, user technology specialist, ITS

Connect with PHX CityofPhoenixAZ

Domestic Violence Awareness Suns Night
Friday, October 5, 2018

ARIZONA COALITION TO END SEXUAL & DOMESTIC VIOLENCE

The Phoenix Suns have partnered with the City, State, County and Local community organizations by hosting a Domestic Violence Awareness game in October the past 5 years.

All 50/50 Raffle proceeds sold during the Suns game will go to the Arizona Coalition to End Sexual & Domestic Violence.

www.acesdv.org

Paint Phoenix Purple - Phoenix Suns - Promotion Link
Promo Code: PPP

Please Contact Sergio Gomez with any questions:
Sergio Gomez
602-262-4946
Sergio.Gomez@phoenix.gov

paintphoenixpurple.org ItCanStop.az.gov