Retired Employees of Los Angeles County

A non-profit organization

March 2024 – "Staying Safer in the Digital World" summary

In this presentation we explain each item to help you stay safer and avoid being scammed

PASSWORDS

- Try to not use shared passwords.
- At least make your email and bank passwords unique.
- Make your passwords memorable-length can be better than overly complex.
- Use a password manager.

WI-FI

- Use only Wi-Fi with passwords.
- Doublecheck Wi-Fi names.
- Turn off Wi-Fi and Bluetooth when not in use (e.g., traveling).
- Use your mobile plan instead.
- "Forget" saved Wi-Fi from hotels and public places.

CARDS

- Lookout for card skimmers—if suspicious, look, jiggle, and pull.
- Use contactless feature if possible, rather than inserting or swiping the card. Swiping is the most risky.
- Use the gas pump or register facing the clerk.
- Use your hand to cover PIN entry.

DIGITAL LIFE

- Share only general information on public social media, if at all.
- Set social media posts to be visible only to friends (and decide if you want "friends of friends).
- Use a fictitious persona for non-legal, financial, governmental, and other websites where real identity does not matter.
- Be on the lookout for phishing email—source address, grammar, layout, etc.
- Backup your data. It's the best tool against ransomware, loss, and theft.

DIGITAL LIFE (Continued)

- Beware of people looking over your shoulder in public places
- Educate yourself about AI "deep fakes".

FINANCIAL LIFE

- Digital cash (Venmo, Zelle) should be sent to friends and known contacts only. Verify account by first sending $1.
- Use credit card where possible, then debit, then checks. Credit cards provide the most protection. Some cards can be credit and debit—ask the merchant to use it as credit.
- Urgent call asking for money is usually fraud.
- When someone calls from the bank, ask for a case number and call back using the number on the back of the card.
- Use Google or Bing to search for a website rather than typing in the address.
- Keep up-to-date pictures of everything in your purse or wallet and sync pictures to the cloud.
- Offer Up, Craigslist, Facebook, etc. are commonplaces for scammers. Do not send money ahead of product. Meet face-to-face when possible.
- Use an identity monitoring service and lock your credit profile with Experian, Equifax, and TransUnion.

DEVICES

- If you travel with your computer, turn on encryption (Bitlocker for Windows and Filevault for Mac).
- Bring your own charger, do not use public chargers.
- Disable iPhone AirDrop and NameDrop.
- Beware of suspicious text messages.
- Guard your devices in public places.

1000 S. Fremont Ave., Unit 15, Alhambra, CA 91803-8802 · Office Hours: Mon.-Thurs. 9:00 a.m. – 3:00 p.m.
(626) 308-0532 · (800) 537-3522 · Fax (626) 308-2901 · www.relac.org · admin@relac.org