Mobile Device Security

Mobile devices (cell phones and tablets) are now integral tools of employees. Most, if not all, of the organization's most sensitive data is now being assessed or stored on these devices. As such, hackers have risen to the challenge of trying to compromise these devices.

WEAC and affiliate organizations have a fiduciary requirement to protect their technology to safeguard members, intellectual property and reputation. WEAC is encouraging the use of Microsoft 365 on the mobile devices to help diminish the impact of the loss of a mobile device. This is extremely important with the upcoming adoption of NEA360, which will enable users to access member's demographic information. Microsoft 365 can enable a user to remotely "clean" a lost or stolen device of sensitive data.

There are additional steps staff and governance can utilize to safeguard their devices.

- Strong password – This is the first defense. Use phrases with numbers and symbols wherever possible.
- Don't click on links in emails without thinking first. Hover over the link to review the web address. Be aware that co-workers or acquaintances email accounts may have been hacked.
- Update your device software when notified of an available update.
- Don't rise to the temptation of clicking on ads on a website.
- Delete unused apps, and update apps that you use on a regular basis. Do not download free software on your PC. Think before downloading free apps that has not been vetted by your device's manufacturer. Android apps are known to be more susceptible to malware than Apple apps due to the open architecture of its operating system. But both operating systems have weaknesses and have had malware issues with approved apps and software.
- Don't use unsecure free Wi-Fi sites when accessing sensitive data.
- Be aware that it takes a combination of firewalls, spam blockers, virus software, malware protection, software updates and common sense to protect your device and our members' data.
- When in doubt, contact the WEAC IT department (zacherj@weac.org or hoffmana@weac.org).

NEA360 Requirements/Recommendations

(see additional requirements in license agreement)

Technical Requirements

1. Devices must use up to date operating systems.
2. Devices must be configured with a secure password or PIN.
3. Review NEA360 Roots – Technology Recommendations to SEA's.

User Recommendations

1. When loading Association data on a mobile device, only load the essential information required. Don't download the birthdates or address of members, if only the work location is needed.
2. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that association data is only sent through the association email system.
3. Users should not use association workstations to backup or synchronize device content such as media files like iTunes, unless such content is required for legitimate business purposes.