*First Things First*

# Conference Security for Participants

FOR ATTENDEES, SPEAKERS AND VENDORS

DO THESE BEFORE, DURING AND AFTER

KEEP IT SIMPLE AND VERIFY AS YOU GO

ELECTION SECURITY *Exchange*

Coalition of Election Association Leaders

A PROJECT OF ELECTION CENTER

Election conferences bring together people with sensitive roles, and hostile actors know it. You do not need to be a security expert to protect yourself and your colleagues. The five habits below are low effort and high impact. They cover your devices, your connection, your visibility, your conversations, and your social media, before you leave, while you are there, and on the way home.

## 1. Keep a low profile in public

**Impact: High** **Effort: Low** **Time: 5 Minutes** **Cost: Free**

### *Why this matters*

A visible badge in a hotel lobby, restaurant, or airport tells anyone watching exactly who you are and what you do. Branded vendor or agency apparel do the same. Harassment, social engineering, and targeting often start with a casual observation in a public space.

### *Do it!*

- Take your badge off the moment you leave the secured conference area.
- Save conference-branded apparel for the conference floor, not for travel or evenings out.
- Do not leave badges, lanyards, or registration materials visible in your car or on a restaurant table.
- Check name tags on luggage and work bags for unnecessary detail.

*Quick check*: Before you step into a lobby, elevator, or restaurant, do a quick badge check. Off and tucked away.

# 2. Go quiet on social media, before and during convenings; be mindful of sharing afterward

**Impact: High** **Effort: Tiny** **Time: Ongoing** **Cost: Free**

## *Why this matters*

Real-time posts ("Just arrived for the conference!") tell hostile actors where you are, who else is there, and most importantly when your home or office is empty. Photos of attendee lists, agendas, badges, or room assignments leak operational details organizers worked hard to protect. Tagged photos from colleagues create the same problem.

## *Do it!*

- Save the posts for after you are home. If you must post during, keep it generic and never live.
- Do not photograph or share attendee lists, room assignments, badges, or detailed agendas.
- Ensure geotagging is turned off in your phone's camera settings.
- Ask colleagues not to tag you in conference posts while the event is active.
- Review your public profiles (LinkedIn, X, Facebook) for details that make you an easy target: direct phone, office address, family information.

***Quick check***: Search your own name on a search engine and on LinkedIn. What can a stranger learn in 60 seconds? Tighten anything that is not essential.

# 3. Protect your screen and your conversations

**Impact: High** **Effort: Low** **Time: Ongoing** **Cost: Free/Low**

## *Why this matters*

Lobbies, hallways, airports, and restaurants are intelligence-gathering environments. A glance over your shoulder, a photo of an open laptop, or an overheard call can expose voter data, vendor relationships, or operational plans. Social engineering often starts with a friendly stranger asking pointed questions.

## *Do it!*

- Lock your screen any time you step away (Windows + L, or Control + Command + Q on Mac).
- Use a laptop and cell phone privacy filter(s) when working in public spaces.
- Keep sensitive calls in your hotel room, not the lobby or hallway.
- Treat unsolicited emails, texts, and calls during the conference with extra suspicion. Verify through a known channel before you act.
- If a stranger asks pointed questions about your office, systems, or colleagues, answer politely but generically.

***Quick check***: Sit in your usual conference seat. Can someone behind or beside you read your screen? If yes, reposition or add a privacy filter.

# 4. Tune up your devices before you travel

**Impact: High**  **Effort: Low**  **Time: 15 Minutes**  **Cost: Free/Low** 

## *Why this matters*

Phones and laptops quietly broadcast more than most people realize. Location services, auto-connecting Wi-Fi and Bluetooth, and outdated software can leak your movements or hand an attacker an opening before you reach the venue. A compromised personal device can expose work accounts, contacts, and conference materials.

## *Do it!*

- Before you travel, update your phone, laptop, browser, and key apps to the latest versions.
- Turn off Bluetooth auto-connect and Wi-Fi auto-join for unknown networks.
- Rename your devices so they do not identify you. “Bob’s iPhone” or “Sally’s AirPods” broadcast over Bluetooth and AirDrop to anyone nearby. Use something generic like “Phone” or “Earbuds” instead.
- Disable location sharing in social apps and review which apps have location access.
- Require a password, or biometric on every device, with a 1 to 2 minute auto-lock.

***Quick check***: Look at your phone lock screen. If a stranger could read your full name, employer, or trip details, scrub it before you travel.

# 5. Lock down your connection

**Impact: High**  **Effort: Low**  **Time: 5 Minutes**  **Cost: Free/Low** 

## *Why this matters*

Hotel, airport, and conference Wi-Fi networks are shared with strangers, and attackers can spoof network names like “Free_Conference_WiFi” to intercept your traffic. Sensitive work (voter data, vendor email, internal documents) should never cross an untrusted network without protection.

## *Do it!*

- Use your phone hotspot for sensitive work whenever you can.
- If you must use Wi-Fi, use a reputable VPN. Your employer may already provide one.
- Verify the official conference network name with staff at registration. Do not guess from the available list.
- After the trip, forget hotel, airport, and conference networks so your devices will not auto-rejoin a spoofed copy on the next trip.

***Quick check***: Open your saved Wi-Fi list. Delete the public networks you no longer need.

Conference security is a team sport. Organizers handle a lot behind the scenes, but the biggest variable is you. Five small habits—tuned-up devices, a secure connection, a low public profile, a protected screen and conversation, and quiet social media—keep the election community safer.