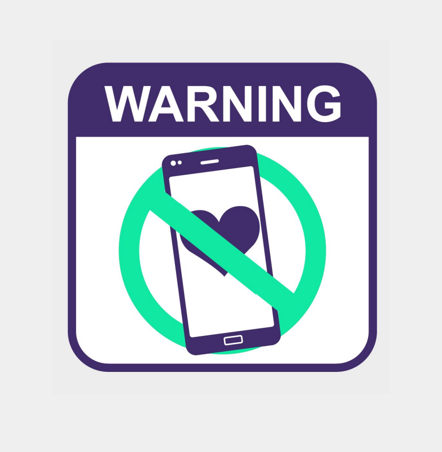
Dating Traps, Catfishing, and Political Espionage



There is a **growing threat** from bad faith actors **targeting civil society, including non-profit employees, teachers, organizers, civil servants, political staff**, and more **via dating apps**. Victims report undercover stings, doctored video, phishing attempts, and other deceptive tactics designed to discredit and intimidate individuals and to threaten the credibility of the organizations they represent.

Below are some tips on how to avoid traps and improve situational awareness, as well as learning to trust your instincts, especially useful in high-risk, uncertain, or unfamiliar settings, such as first dates, travel, protests, or political meetups.

Why You Might Be A Target

1. **Your job gives you access to sensitive financial or security information.**
   - Why it matters: Access to donor data, advocacy or campaign strategies, security plans, staffing information, or other insider information makes you a high-value target for infiltration, phishing, or manipulation.
2. **You are a publicly visible figure.**
   - Why it matters: Your visibility makes you easier to track and impersonate, and also increases the impact of disinformation or blackmail efforts aimed at discrediting you or your organization.
3. **You work on a divisive subject or issue.**
   - Why it matters: Movements related to abortion access, police accountability, climate action,
   - LGBTQ+ rights, immigration, or labor are frequent targets of surveillance, infiltration, and sabotage due to their political sensitivity.
4. **Your work, issue, or organization has been garnering press attention.**
   - Why it matters: Increased media coverage draws attention from adversaries—state actors, opposition campaigns, or extremist groups—who may view your organization as influential or disruptive and seek to gather intelligence or disrupt operations.
5. **You have minimal security support.**
   - Why it matters: Lack of infrastructure, like vetted protocols, digital security, or trained staff, makes it easier for bad actors to exploit gaps in awareness, impersonate allies, or collect data unnoticed.

Dating Traps, Catfishing, and Political Espionage

Before Meeting

1. Minimize The Personal Information You Share

- Avoid sharing your full name, address, workplace, or other details that can identify you.
- Don't use photos that also appear on your personal social media account and networking accounts.
- Strip meta or geolocation data tracking home, work, or family addresses.
- Don't link dating apps to other social media accounts.

2. Protect Your Data Accounts

- Use Different, Strong Passwords and 2-Factor Authentication for your various accounts. Do not use the same password used for your online dating account on other accounts.
- Enable 2-factor authentication (2FA) for dating apps and associated email accounts

3. Check The Digital Footprint of Your Potential Date

- Research your matches with a cursory search of their social media to make sure their story is consistent. Watch for recently created accounts, vague affiliations, or strangely polished profiles.
- Look for inconsistencies between what they say and what's publicly available.
- Stay within the platform's messaging system until you feel comfortable sharing other contact information.
- Use Google Voice as a phone number to connect with folks until you feel comfortable sharing your real phone number.
- If potential dates are asking for money, gift cards, or financial information, proceed with caution. This is a sign of a scam.

4. Monitor The Conversation

- Ask specific, low-stakes questions. Probe gently about their background, mutual contacts, or local context. See if their answers match known facts or feel evasive or overly generic.
- Take note if your match is asking detailed questions about your work, professional history, donor information, or other proprietary information about your organization or your colleagues. This can be a sign of a trap.
- Watch for "eager but vague" behavior. People doing political surveillance often seem overly enthusiastic and can be hyper-specific with their questions. Be cautious if they mirror your views too perfectly or push to meet in-person quickly.

5. Trust Your Instincts

- Don't feel pressured to connect with everyone.
- Know when to walk away. If something feels off, that is enough to end the conversation.
- If a profile seems suspicious, like very limited information, overly perfect photos, or inconsistent details, proceed with caution or unmatch/block them.

Meeting Up

1. **Choose the Setting With Surveillance in Mind**
   - Meet somewhere well-lit, public, but noisy—like a busy café or bar, bookstores, or a public park—where hidden mics or discreet recordings are harder to pull off. Avoid locations where you'd feel pressured to talk privately or reveal sensitive information.

2. **Scan the Space When You Arrive**
   - Take 10 seconds to notice exits, sightlines, cameras, and chokepoints. Mentally note who's coming and going, where the crowded vs. quiet areas are, and where you'd go if something felt off.

3. **Clock the "Mood of the Room"**
   - Is the energy tense, relaxed, nervous, or too quiet? Subtle shifts in tone, body language, or conversation volume can signal trouble before anything explicit happens. Trust that vibe check.

4. **Watch for Behavioral Red Flags**
   - Take note if they repeatedly try to steer the conversation away from themselves or towards your work dynamics, security, or financial information, or specific individuals you work with.

5. **Pay Attention to the "Off" Feeling**
   - If something feels strange—too scripted, too fast, too familiar—it probably is. You don't need to explain that feeling to act on it. Slow down, exit, or change topics without apology.

6. **Practice Noticing Small Details**
   - Challenge yourself to remember things like clothing colors, tattoos, license plates, or group formations. Watch for cameras or phones taking videos nearby. Sharpening your observation muscles makes it easier to spot what doesn't belong.

Dating Traps, Catfishing, and Political Espionage

Getting Home Safely

1. **Give Yourself Permission to Bail**
   - Whether it's a meeting, date, or event—leaving early doesn't make you rude or weak. Your safety is more important than social expectations. You get to decide when a situation is making you feel uncomfortable or unsafe and how you proceed. Have an exit plan, and rehearse saying "Gotta run, I'll text you later."

2. **Tell A Friend**
   - Let a trusted member of your community know where you are and who you intend to meet. Develop a plan for what you want this person to do if they don't hear from you by the agreed-upon time.

3. **Report Out**
   - Share your ride to and from the location if you are using Uber or Lyft with a trusted member of your community, or generally share your location with them until you return home.

You Suspect You Were The Victim of a Trap

1. Let a member of your trusted circle, including family, friends, and a member of your team, know about the interaction.

2. Share your suspicions with your employer so that they can make a plan or attempt to stop any public action by hostile actors.

3. Cease any further contact with the individual and block their ability to reach you.
   Document and save any interactions that may have raised suspicion, including texts, emails, or messages within the app.

A Staff Member Suspects They Were The Victim of a Trap

When a staff member reports that they may have been the victim of a trap, here are some reminders and tips to follow.

1. Don't panic or make any public statements immediately until you learn all the facts.
2. Provide immediate support to your staff member. Don't blame or penalize the victim.
3. Engage legal counsel or outside advisors, like a crisis communications firm, to support your team.
4. Notify your crisis comms team or develop one if you don't have one in place.
5. Have that communications team draft a holding statement.
6. Run a quick internal review of what information may be at risk.
7. Begin monitoring public channels for signs of disinformation or videos posted.