FLUXLABS

GUIDE · MUNICIPALITIES

Security basics for city staff

Cities hold records, money and services residents depend on, which makes them a favorite target. Every employee is part of the defense.

Why cities get targeted

- Public email addresses and staff names make scam emails easy to aim.
- Payments to vendors and contractors are attractive to payment fraud.
- Service outages put pressure on a city to pay a ransom quickly.
- Email and records may be public, so scammers can study how you work.

Everyday habits

Do

- ✓ Lock your screen every time you step away
- ✓ Use two-step sign-in and never approve a prompt you didn't start
- ✓ Call vendors on a known number before changing payment details
- ✓ Report strange emails, calls and pop-ups right away
- ✓ Keep work on city devices and city accounts

Don't

- ✗ Share sign-ins at the front counter or between shifts
- ✗ Plug in USB drives from the public or vendors
- ✗ Use personal email for city business
- ✗ Let a visitor use a staff computer
- ✗ Ignore an alert because "IT will see it"

Public records and email

- Assume anything you write in city email may become a public record. Keep it professional.
- Don't move city business to text messages or personal accounts. It may still be a record, and it's not protected.
- Ask your clerk before deleting email that might be a record.

Scams aimed at cities

1. **Fake vendor payment changes.**
   A contractor's "new bank account". Always call the vendor on a number already on file.
2. **Fake resident or records requests**
   with attachments or links. Open them only through your normal records system.
3. **Fake calls from "IT" or the state.**
   Hang up and call back on a number you know before giving access or codes.
4. **Urgent requests from an official.**
   A council member or the manager asking for money or gift cards by email is a scam.

> **Something looks wrong?**
> Call your IT support before you click, pay or reply. Forward odd emails to **check@scan.fluxlabs.net** for a free verdict.