TODOSECURE

PROTECTING YOUR BUSINESS, BYTE BY BYTE

Quick-Action Prevention Checklist for Small-Business Owners

1. **Run Weekly "Security Moments"**
    - Set aside 5-10 minutes each week to discuss a recent social-engineering example (e.g., a phishing email or a tailgating incident).
    - Encourage staff to ask "What would I do?" and reinforce the "verify before you comply" rule.
2. **Verify All Unsolicited Requests**
    - **Phone calls:** Hang up and call the organization back using a known, official number.
    - **Emails/texts:** Hover over links, check the sender's address, and confirm via a separate channel (e.g., a known corporate email or phone).
    - **In-person visitors:** Ask for photo ID, check the visitor log, and never let strangers hold doors open for you.
3. **Lock Down Physical Access**
    - Install visitor-sign-in sheets or electronic badge readers.
    - Issue temporary badges that expire at the end of the day.
    - Keep doors closed; never prop them open for anyone you don't recognize.
4. **Shred Sensitive Paper**
    - Use a cross-cut shredder for invoices, contracts, payroll sheets, and any document containing personal or financial data.

- Store remaining paperwork in locked cabinets until it can be shredded.

5. **Enable Email & Phone Filtering**
    - Activate spam/phishing filters on your email gateway.
    - Block unknown or suspicious phone numbers on office landlines and mobile devices.
    - Teach staff to “hover” over links and attachments before clicking.
6. **Create a Simple Reporting Channel**
    - Set up a dedicated email address (e.g., security@yourcompany.com) or a short online form for staff to report anything odd.
    - Assign a point person (or small team) to review reports within 24 hours and take immediate action if needed.
7. **Backup Critical Data Regularly**
    - Perform automated daily backups to an offline or cloud location you control.
    - Test restoration procedures quarterly to ensure backups are usable.
8. **Limit Privileged Access**
    - Apply the principle of least privilege: give employees only the access they need for their role.
    - Review permissions quarterly and revoke unused accounts promptly.
9. **Use Multi-Factor Authentication (MFA)**
    - Enable MFA on all business-critical accounts (email, banking, cloud services).
    - Prefer authenticator apps or hardware tokens over SMS where possible.
10. **Stay Informed**
    - Subscribe to a trusted security newsletter (e.g., Proton’s blog, US-CERT alerts).
    - Periodically review the latest social-engineering trends so you can adapt your defenses.

www.todosecure.net

info@todosecure.net

210-560-3992