Nametag

Workforce Impersonation Risk Checklist

Attackers are increasingly gaining access by impersonating employees, contractors, or executives in everyday workflows like hiring, account recoveries, helpdesk-driven support interactions, and access requests.

Use this checklist to quickly spot where impersonation risk may exist across your workforce. Check the boxes that apply to your organization.

Hiring & Onboarding

- [ ] We rely on video interviews to confirm candidate identity
- [ ] Background checks don't confirm the candidate is the person interviewed
- [ ] IT issues credentials and devices without verifying the real person

Account Recovery & Helpdesk

- [ ] Helpdesk verifies users using personal or account information (i.e. security questions)
- [ ] MFA or password resets can be approved without identity verification
- [ ] Video calls are used as a primary method to verify employees

Access & Privileges

- [ ] Privilege or role changes don't require identity verification
- [ ] Admin access can be approved based on tickets or chat requests

Approvals & Finance

- [ ] Executives approve payments or sensitive actions via email, chat, or calls
- [ ] There's no way to verify the person behind high-risk approvals

AI & Automation

- [ ] AI agents can perform actions without verified human approval
- [ ] Agent actions aren't clearly tied back to a real person

If you checked multiple boxes, your organization may have an identity assurance gap — places where access is granted without verifying the real person behind the request.

Nametag helps teams reduce impersonation risk by verifying people during high-risk actions like account recovery, onboarding, and access changes.

contact us: sales@nametag.co
visit us: getnametag.com

Learn More