

OWNERS & EXECUTIVES

Owner & Executive Digital Protection Checklist

Owners, finance staff, and executives are the people attackers impersonate and target first. A few rules stop the most expensive scams, including business email compromise and AI voice cloning.

Stop payment fraud

- ☐ Never change bank or payment details based on an email, text, or call alone; call back on a number you already have
- ☐ Require two people to approve new payees, bank changes, and large or urgent payments
- ☐ Agree on a code word with family and key staff to verify urgent requests, since voices and video can now be faked with AI
- ☐ Treat urgency, secrecy, and gift-card requests as red flags, especially when they appear to come from you

Harden the accounts that matter most

- ☐ Use phishing-resistant MFA (passkeys or security keys) on email, banking, payroll, and your domain registrar
- ☐ Keep account recovery email addresses and phone numbers current, and store recovery codes offline
- ☐ Use delegated access for assistants instead of sharing your password
- ☐ Use separate administrator accounts for IT changes, not your everyday email login

Reduce what attackers can learn

- ☐ Search for yourself and your company: note exposed emails, org charts, home address, and family details
- ☐ Limit public staff directories with direct emails and reporting lines; use role addresses such as info@
- ☐ Be careful what you post about travel while you are away

Travel

- ☐ Bring only the devices you need; consider a loaner laptop and phone for high-risk travel
- ☐ Use your own charger and a wall outlet rather than public USB charging ports
- ☐ Use your phone's hotspot instead of hotel or airport Wi-Fi for sensitive work
- ☐ Update and fully back up devices before you leave

Sources and further reading

Nexus: Deepfake and voice-clone verification checklist (PDF):

<https://www.nexussecurityadvisors.com/nexus-deepfake-verification-checklist.pdf>

Nexus: Spotting AI fakes: <https://www.nexussecurityadvisors.com/ai-detection>

FBI Internet Crime Complaint Center (IC3): <https://www.ic3.gov/>

Need help rolling this out across your team? Request a consultation at [nexussecurityadvisors.com/get-started](https://www.nexussecurityadvisors.com/get-started).