



CHECKLIST

Cybersecurity Readiness Guide for Business Leaders

No employee needs to become a cybersecurity expert to protect your business. They need three habits, repeated until they're automatic: recognize when something looks unusual, verify it through a channel you already trust, and report it right away, without hesitation. Use this checklist to see where your team already has those habits in place, and where a gap still needs closing.

Simulated Phishing Tests

- ☐ Employees receive phishing simulation training at least once a year, covering phishing, business email compromise, and password practices.
- ☐ New employees receive initial cybersecurity training within 10 days of their start date.
- ☐ Simulated phishing tests vary in difficulty and tactic over time, rather than repeating the same obvious template.
- ☐ Results are used to identify who needs follow-up coaching, not to single out or penalize employees who click.

Suspicious Calls & Messages

- ☐ Employees know that phone calls and text messages deserve the same scrutiny as email, not less.
- ☐ Any request to change payment details, account information, or wiring instructions is verified through a secondary channel, such as a callback to a known number, before action is taken.
- ☐ Employees are told never to use contact information provided in the suspicious message itself to "verify" it.

Executive & Vendor Impersonation

- ☐ Employees know that an urgent, off-process request (a gift-card purchase, a rushed wire transfer, a sudden change in tone) is a signal to slow down, not speed up.
- ☐ A standing rule exists: no financial request is completed based on a message or call alone, regardless of who it appears to be from.
- ☐ Employees understand that a convincing voice or video is not proof of identity, and know to hang up and call back on a known number if anything feels off.
- ☐ A shared code word or phrase, set up in person or on a verified call and never sent by text or email, is required to confirm identity for high-stakes requests from executives or vendors.

Unexpected MFA Requests

- ☐ Employees are told that an MFA prompt they did not generate themselves should be denied and reported immediately, never approved to “make it stop.”
- ☐ Repeated, unexpected MFA prompts are treated as evidence a password may already be compromised, not a technical annoyance.
- ☐ Where possible, number-matching or phishing-resistant MFA is in place to reduce the effectiveness of push-bombing attempts.

Fraudulent QR Codes & Login Pages

- ☐ Employees are told not to scan QR codes from unknown senders, unsolicited packages, or unfamiliar flyers and posters.
- ☐ Before entering a password anywhere, employees check that the web address matches what they already know, not just the page’s logo or design.
- ☐ IT has a clear, known way for employees to report a suspicious QR code or login page without needing to diagnose it themselves first.

Information-Sharing Guidelines

- ☐ Employees know that small operational details (an org chart, a travel schedule, a vendor name, an invoice format) can be combined by an attacker into a convincing pretext.
- ☐ Requests for this kind of information from an unverified caller or sender are met with a pause and a verification step, not an automatic answer.
- ☐ Employees understand this is about pausing to verify, not refusing to be helpful.

Incident Reporting & Escalation

- ☐ Every employee knows exactly who to contact, and how, the moment they suspect they clicked a bad link, entered credentials somewhere they shouldn’t have, or approved something they didn’t request.
- ☐ The reporting process has been tested or rehearsed within the last year, not just written down and filed away.
- ☐ Reporting a mistake is treated as the right call, not a disciplinary event, so employees report in minutes rather than staying quiet and hoping nothing comes of it.

If this checklist turned up more open boxes than closed ones, that’s a normal starting point, not a verdict. If you need support putting any of this into practice, we’re here to help at every step.

Contact us, and let’s get started.