BROTHERLY TECHNOLOGY

SECURITY CULTURE CHECKLIST

10 Steps to Build a Cyber-Smart Team

A practical framework for turning security awareness into daily habits instead of a once-a-year training you check off and forget.

01	**10 concrete steps that build company-wide security habits, not just an annual training**
02	**How to run phishing simulations that coach employees instead of shaming them**
03	**Ways to make reporting suspicious activity easy, fast, and blame-free**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

BROTHERLY TECHNOLOGY

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] Employees get interactive, scenario-based training tied to real job tasks - not an annual slideshow.	[ ] Yes [ ] Partial [ ] No
[ ] Cybersecurity comes up in regular team conversations, not only after something goes wrong.	[ ] Yes [ ] Partial [ ] No
[ ] Phishing simulations run on a schedule, with results used to coach, not to publicly call anyone out.	[ ] Yes [ ] Partial [ ] No
[ ] Training connects protecting company data to protecting employees' own personal information.	[ ] Yes [ ] Partial [ ] No
[ ] Leadership visibly follows the same MFA, password, and device rules everyone else does.	[ ] Yes [ ] Partial [ ] No
[ ] Security guidelines are written in plain language and reviewed at least once a year.	[ ] Yes [ ] Partial [ ] No
[ ] Training is tailored by role, since finance, HR, and executives face different real-world scams.	[ ] Yes [ ] Partial [ ] No
[ ] Employees understand how their individual actions affect the whole company's exposure.	[ ] Yes [ ] Partial [ ] No
[ ] Staff know exactly how and where to report something suspicious, without extra steps.	[ ] Yes [ ] Partial [ ] No
[ ] Nobody hesitates to report a mistake for fear of blame or embarrassment.	[ ] Yes [ ] Partial [ ] No
[ ] Good security behavior gets recognized - a shout-out or note, not just silence.	[ ] Yes [ ] Partial [ ] No
[ ] A named owner reviews and updates the security-awareness program at least annually.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

CULTURE BASELINE

Turn each step into a practice you can measure

A security-aware culture isn't one training session. It's a small set of habits, reinforced consistently, with someone accountable for keeping them alive.

Habit	What it looks like in practice	Evidence
Training	Interactive, scenario-based modules tied to real job tasks	Completion rate and scores by department
Communication	Security is a standing agenda item, not a once-a-year email	Meeting notes and channel activity
Readiness testing	Scheduled phishing simulations with private coaching	Click/report rates trending down over time
Role-based guidance	Finance, HR, and execs trained on the scams that target them specifically	Role-specific modules completed
Leadership example	Leaders use MFA, a password manager, and approved tools like everyone else	Admin/exec accounts match written policy
Reporting culture	Reporting suspicious activity is fast, easy, and blame-free	Report volume and time-to-report trend up

None of these rows require new software. They require one named owner and a recurring review on the calendar.

MAKE IT STICK

Five steps to launch or refresh the program

Most security-awareness programs fail from neglect, not design. These five steps build a cadence you can actually sustain.

1	Name one owner for the security-awareness program - not 'IT in general.'
2	Run a baseline phishing simulation before announcing any new training, so you have a real starting number.
3	Launch short, role-based training modules and schedule the next simulation 60 to 90 days out.
4	Publish plain-language security guidelines and put reporting instructions where employees actually look.
5	Build recognition and results review into a recurring quarterly check-in, tied to the evidence above.

What to watch for

WATCH: Training is a single annual video nobody remembers by March.

WATCH: Nobody can name who owns the security-awareness program.

WATCH: Phishing test results are used to publicly call out individual employees.

WATCH: Employees say they wouldn't report a mistake because of how the last one was handled.

WATCH: Executives are exempt from the same rules everyone else follows.

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	_____
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	_____
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	_____
NEXT QUARTER	Test the process, document results, and assign improvements.	_____

Notes / decisions / questions for your provider

_____

_____

_____

_____

_____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: CISA Secure Our World: cisa.gov/secure-our-world | SANS Security Awareness: sans.org/security-awareness-training

This guide is educational and is not legal, regulatory, tax, or insurance advice. Confirm requirements and pricing for your organization with qualified advisors and vendors.