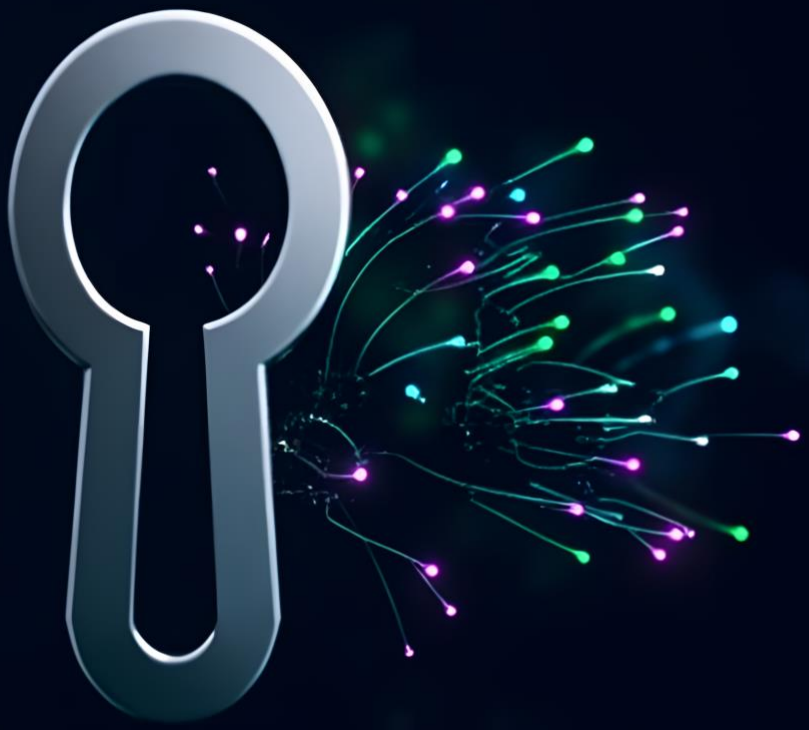
Hacker® SIMULATIONS



CORE 4 CYBERSECURITY CHECKLIST

Steps to Protect your Business and your People

1. Strengthen Passwords & Use Multi-Factor Authentication (MFA)

Why it Matters:

Weak or reused passwords cause over **60% of data breaches**. Adding MFA can block more than **99% of automated attacks**.

Checklist:

☐ Enforce minimum password length (12+ characters)
☐ Require mix of upper/lowercase, numbers & symbols
☐ Prohibit password reuse across systems
☐ Roll out a **password manager** to your team (e.g., 1Password, Bitwarden)
☐ Enable **MFA** on:

- Email accounts (Microsoft 365, Google Workspace)
- VPN / remote access
- Cloud platforms (AWS, Azure, Salesforce, etc.)

☐ Train staff on recognizing MFA fatigue or prompt bombing attacks

Pro Tip: Start with executives and finance teams, they're top targets for account compromise.

2. Update & Patch Systems Regularly

Why it Matters:

Hackers rely on **known vulnerabilities** that already have fixes, they win when you **delay**.

Checklist:

☐ Turn on **automatic updates** for all OS & software
☐ Schedule regular **patch windows** (weekly or monthly)
☐ Keep browsers, plugins, and mobile apps updated
☐ Remove or disable outdated, unused software
☐ Apply firmware updates for routers, firewalls, and IoT devices
☐ Maintain an **asset inventory** so nothing is missed

Pro Tip: Use centralized update management tools (Intune, WSUS, or MDM) to simplify patching.

3. Think Before You Click, Phishing & Social Engineering

Why it Matters:	Checklist:
Most breaches start with a single **human click**. Awareness saves **time**, **money**, and **reputation**.	☐ Train employees to spot red flags: • Urgent requests, misspellings, strange links • Sender addresses that don't match the domain ☐ Simulate phishing attacks quarterly ☐ Create a clear "**Report Phish**" button or channel ☐ Verify financial requests *verbally* or via a second channel ☐ Limit public info that reveals org structure or executive contacts

Pro Tip: Make reporting easy and praise those who catch phishing attempts, don't shame clicks, coach them.

4. Back Up & Protect Your Data

Why it Matters:	Checklist:
If ransomware hits or files are corrupted, **backups** can be the difference between **recovery** and ruin.	☐ Follow the **3-2-1 rule:** • 3 copies of data • 2 different storage types • 1 copy offsite (offline or cloud) ☐ Test restores monthly ☐ Encrypt backups at rest and in transit ☐ Restrict backup access to admin-only ☐ Automate backup schedules where possible ☐ Document your disaster recovery plan

Pro Tip: A backup you can't restore is just storage. Always test your restore process.

BONUS: Build a Cyber-Aware Culture

Why it Matters:	Checklist:
Because technology isn't enough.	☐ Appoint a security champion or internal ambassador ☐ Run monthly micro-trainings or 5-minute awareness tips ☐ Post security reminders in internal comms (Slack, Teams) ☐ Celebrate wins, "Zero Phish Month" challenges or quizzes

Pro Tip: Cybersecurity isn't a one-time project. It's a daily habit that protects your team, your customers, and your brand.

Want to go further?

Free 30 min Security Triage Call

10% of our Pentesting Services

Complimentary Phishing Simulation for existing clients

BOOK NOW >

FIND, FIX, FORTIFY

www.hackersimulations.com
info@hackersimulations.com
(+1) 833 608-2662
New York, NY, USA

Hacker® SIMULATIONS

5.0/5.0