



Cybersecurity Self-Check

Take this quick self-check to see how your security habits measure up. No jargon, no stress. Just 10 questions that reveal where you may be at risk. Once complete, share your filled-out assessment with a Zeta Sky representative. They'll walk you through your score and what it means for your security.

Multi-Factor Authentication (MFA)

Adding a second layer of verification is one of the simplest ways to reduce the risk of a breach. The question is how consistently it's applied across your business.

1: How is MFA used in your business today?

- On critical systems and for remote access
- On most apps and administrator accounts across the business
- Only for email or one application

2: How often do you review or adjust MFA settings?

- Adjustments are made when someone leaves the company or changes devices.
- Reviews usually happen during scheduled audits, sometimes more if needed.
- MFA settings stay the same unless something breaks or stops working.

Password & Identity Management

Weak or reused passwords are still one of the most common ways attackers get in. A strong approach makes things easier for employees while closing easy gaps.

3: How do employees usually handle passwords?

- Passwords are created by employees, and some end up being reused across accounts.
- There are company rules in place, though they may not always be followed consistently.
- A secure password manager is available and used by most staff.

4: When someone leaves the company, what happens to their accounts?

- IT usually steps in to remove accounts, though timing can vary depending on workload.
- Some accounts stay open longer than expected before being fully closed.
- Access is often removed quickly, sometimes automatically depending on the system.

Cyber Awareness Training

Technology is only part of security. People are often the first target, which makes training and awareness just as important as firewalls.

5: How often do employees receive cybersecurity training?

- Training is included during onboarding, with limited follow-up afterward.
- Employees receive sessions annually, and sometimes additional refreshers.
- Training is delivered on a regular basis, and phishing simulations are used to test awareness.

6: If an employee gets a suspicious email, what's most likely?

- Some employees report these messages, while others might dismiss them without action.
- Staff are generally confident in recognizing phishing attempts and know how to escalate them.
- It's possible an employee could mistake the email as legitimate and interact with it.

Email Security

Email is one of the most common entry points for attackers. Filtering, scanning, and quarantine tools can stop most threats before they hit an inbox.

7: How does your team handle phishing emails?

- Filtering tools block most suspicious messages, although some still reach inboxes.
- Employees tend to delete suspicious emails when they notice them.
- Threats are often caught by multiple layers of filtering, including link scanning and quarantines.

8: How often are email security settings reviewed or updated?

- Reviews typically take place during major IT updates or system changes.
- Settings are checked on a routine basis to stay aligned with evolving threats.
- Reviews happen infrequently and may only occur when something breaks.

Zero Trust Security

Instead of assuming everything inside your network is safe, Zero Trust checks every user, device, and app, every time. This limits the damage an attacker can cause if they get in.

9: How much access do employees have once they log in?

- Employees can get into many different systems once they're logged in, even those not tied to their role.
- There are rules around access, though enforcement may not always be consistent.
- Access is usually tied to job responsibilities, with employees only seeing what they need.

10: How often are devices and apps checked for security?

- Devices are generally trusted once they connect, with little follow-up afterward.
- Reviews typically happen during setup and may be revisited about once a year.
- Security checks are performed whenever a device or app attempts to connect.

Business Continuity & Data Protection

When incidents happen, recovery speed determines how much disruption your business experiences. Backup and recovery practices are a key part of cybersecurity strength.

11: How often is your business data backed up and verified for recovery?

- Backups happen after major updates or when IT has time to run them.
- Backups are performed on a set schedule, with recovery tests happening occasionally.
- Automated backups run frequently, and restoration tests confirm data can be recovered when needed.

12: If a system outage or cyberattack occurred, how quickly could operations resume?

- Recovery would depend on IT availability and the nature of the disruption.
- A recovery plan is in place and has been tested in drills to ensure business continuity.
- The plan exists, but the team hasn't tested it recently or may not know all the steps.

Your Cybersecurity Score

Share your completed self-check with a Zeta Sky representative to see your exact score and learn how to strengthen your defenses.

12 – 18 points: Significant Gaps

Your business faces serious risks that could disrupt operations and client trust. Building a stronger foundation is urgent. Partnering with a trusted provider like Zeta Sky ensures these gaps are addressed quickly and effectively.

19 – 28 points: Progress With Weak Spots

You've taken steps in the right direction, but weaknesses remain that could undermine your progress. Working with a partner like Zeta Sky helps close those gaps, simplify your security, and give you peace of mind.

29 – 36 points: Strong, But Never Finished

Your defenses are ahead of many peers, yet cybersecurity never stands still. Continuous improvement and expert oversight are essential. Partnering with a team like Zeta Sky helps ensure your business stays resilient and prepared for the future.

