LastPass •••|

Are You Prepared for the Most Common Cyber Risks? A Checklist

Preventing cyber risks requires a well-executed security strategy emphasizing employee education, a strong cyber culture, and effective technology.

Here's a checklist that offers a starting point for preventing the most common cyber risks:

MALWARE

Careless employees and gaps in security can lead to malware.

To prevent its damaging effects:

- [ ] Apply updates and patches to software and systems.
- [ ] Educate employees on the dangers of suspicious links.
- [ ] Restrict admin accounts with strong passwords, MFA, and privilege-based security policies.
- [ ] Deploy antivirus and antimalware software.

RANSOMWARE

Malware prevention is key to stopping ransomware.

To mitigate the impact of a ransomware attack:

- [ ] Back up company data regularly and automate where possible.
- [ ] Store backups on separate networks/ devices or at a data center with redundancy.
- [ ] Create an incident response plan for detecting and responding to an attack.
- [ ] Deploy firewalls and endpoint protections.

PHISHING

Though many phishing attempts are easily spotted, some can be highly sophisticated and targeted for maximum effectiveness.

To stop employees from falling victim to phishing:

- [ ] Require anti-phishing training for all employees and repeat annually.
- [ ] Enable MFA for employee accounts and corporate networks.
- [ ] Use pop-up blocking technology.

PASSWORD ATTACKS

Bad passwords remain a leading cause of data breaches.

To improve password security:

- [ ] Add a password policy to the employee handbook.
- [ ] Educate employees about password security and repeat training annually.
- [ ] Enforce secure passwords and storage with a password manager.

LastPass can help prevent the most common cyber attacks.

Learn more

LastPass •••|