Cybersecurity Checklist

Get started down the path of becoming a cyber-resilient organization with these tips.

Do's

- ☐ **Update software:** Regularly update operating systems, applications, and security software to patch vulnerabilities.
- ☐ **Use strong, unique passwords:** Use complex passwords and consider a password manager to generate and store them securely.
- ☐ **Use Multi-Factor Authentication (MFA):** Enable MFA for all accounts and systems for an extra layer of security.
- ☐ **Backup regularly:** Maintain backups of critical data and ensure they're stored securely, preferably off-site.
- ☐ **Educate employees:** Conduct regular cybersecurity training on phishing, social engineering, and other threats.
- ☐ **Install firewalls and antivirus:** Install and maintain firewall and antivirus software to protect against malware and unauthorized access.
- ☐ **Limit access:** Limit user access to only necessary systems and data to reduce the attack surface.
- ☐ **Have an incident response plan:** Develop and practice a clear plan for responding to security incidents, including reporting and mitigation.
- ☐ **Monitor:** Implement monitoring tools and maintain logs to detect and respond to suspicious activities.
- ☐ **Secure Wi-Fi networks:** Use strong encryption and change default passwords for Wi-Fi networks.
- ☐ **Conduct security audits:** Conduct periodic security assessments and penetration tests to identify and address vulnerabilities.
- ☐ **Encrypt data:** Encrypt sensitive data in transit and at rest to protect against interception and unauthorized access.

Don'ts

- ☐ **Suspicious links:** Avoid clicking on links or downloading attachments from unknown or unverified sources.
- ☐ **Security warnings:** Take security warnings seriously and don't bypass them without proper validation.
- ☐ **Sensitive information:** Avoid sharing confidential information through unsecured channels, especially email.
- ☐ **Default passwords:** Never use default passwords for any devices or accounts; always change them.
- ☐ **Reusing passwords:** Avoid using the same password across multiple accounts or systems.
- ☐ **Security updates:** Do not disable or postpone software updates – they often contain critical security patches.
- ☐ **Unknown email attachments:** Avoid opening attachments or downloading files from unfamiliar or suspicious emails.
- ☐ **Unsecured networks:** Avoid accessing sensitive information over public or unsecured Wi-Fi networks.
- ☐ **Social engineering attempts:** Be cautious of unsolicited requests for sensitive information, even if they appear legitimate.
- ☐ **Employee training:** Don't overlook the importance of ongoing cybersecurity training for employees.
- ☐ **Mobile device security:** Ensure mobile devices are protected with strong passwords, encryption, and security software.
- ☐ **Regular audits:** Don't skip regular security audits, as they are essential for identifying and addressing vulnerabilities.

Implementing these do's and avoiding these don'ts will significantly enhance your organization's cybersecurity posture and help protect against cyber threats. Contact us today if you need help with your cyber resiliency plan.

tidalbasingroup.com
675 N. Washington Street – Suite 400, Alexandria, VA 22314
T: 888.282.1626

TB TECHNOLOGIES