View as Webpage

Strengthening Your Business's Cybersecurity

In today's digital world, safeguarding your business against cybersecurity threats is more important than ever. With threats such as ransomware, phishing attacks, and data breaches on the rise; it's crucial to implement best practices to protect your business and customer data. Below are effective tips and strategies, curated from trusted sources like the Federal Communications Commission (FCC) and the Cybersecurity & Infrastructure Security Agency (CISA), to help you strengthen your business's cybersecurity defenses.

---

1. Foster a Culture of Security

- Cybersecurity is not just an IT responsibility; it's a company-wide priority. Business leaders should promote a culture of security by communicating its importance regularly, setting clear security goals, and leading by example.
- Appoint a Security Program Manager to oversee your cybersecurity strategy, track progress, and conduct regular updates to ensure alignment across your organization.

2. Train Your Employees

- Conduct regular training to educate employees on security principles, such as identifying phishing attempts, creating strong passwords, and adhering to safe internet practices.
- Establish clear policies on handling sensitive data, internet usage, and reporting suspicious activities.

3. Implement Strong Access Controls

- Assign individual user accounts for employees with role-specific access to minimize exposure.
- Use multi-factor authentication (MFA) to add an extra layer of protection to your systems, especially for email and administrator accounts.
- Regularly review and update access permissions.

4. Protect Your Technology

- Keep all software, operating systems, and web browsers up to date with the latest security patches.

- Install and maintain antivirus software to defend against malware and viruses.
- Enable firewalls to block unauthorized access to your networks and ensure employees working remotely have similar protections.

5. Secure Mobile Devices

- Develop a mobile device action plan requiring password protection, data encryption, and the use of security apps.
- Set protocols for reporting lost or stolen devices promptly to minimize potential breaches.

6. Backup Your Data

- Regularly back up critical business data, including financial records, customer information, and operational documents.
- Store backups securely offsite or in the cloud, and periodically test data restoration to ensure reliability.

7. Safeguard Payment Systems

- Use the most secure and validated anti-fraud tools available for payment processing.
- Using Oak Bank's Positive Pay service will help reduce fraud.
- Isolate payment systems from less secure programs and avoid using the same devices for payment processing and general web browsing.

8. Conduct Cybersecurity Drills

- Host tabletop exercises to simulate potential cyberattacks and test your incident response plan (IRP).
- Use these exercises to identify gaps and improve your preparedness.

9. Monitor and Maintain Your Systems

- Regularly test your backups, patch vulnerabilities, and monitor for unusual activity.
- If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted and hidden.

10. Create and Use an Incident Response Plan (IRP)

- Develop a written IRP outlining steps to take before, during, and after a cyber incident.
- Involve leaders across departments and review the plan regularly to ensure it's current and effective.

Going beyond the basics.

Besides these basic steps, and to learn details about the steps above, visit these websites: US Small Business Administration - Strengthen Your Cybersecurity , Federal Communications Commission - Cybersecurity for Small Businesses, and Cybersecurity & Infrastructure Security Agency (CIBA) - Cyber Guidance for Small Business.

Together, let's take proactive measures to safeguard our businesses and communities from cyber threats.

For additional security information, you can visitOak Bank's Security Information on our website.

Need help with your account?

Email: bank@oak.bank
Call: 608.441.6000

If your Oak Bank Debit/ATM Card has been misplaced, call 877.755.2957.

If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

VISIT OAK BANK ONLINE

608.441.6000
877.625.2265 Toll Free

Lobby
M - F: 8 a.m. - 5 p.m.

Drive-up
M - F: 8 a.m. - 5 p.m.

Member FDIC

Oak Bank NMLS #434669